

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA**  
Norfolk Division

CENTRIPETAL NETWORKS, LLC,  
Plaintiff,

v.

Civil Action No. 2:18-cv-00094 (EWH)

CISCO SYSTEMS, INC.,  
Defendant.

**MEMORANDUM OPINION AND ORDER**

This is a patent infringement case with an unusual history. Commencing in May 2020, this Court held a six-week bench trial via the Zoom platform during the height of the COVID-19 pandemic. Before the Court issued its post-trial findings of fact and conclusions of law, Defendant Cisco Systems, Inc. (“Cisco”) moved for recusal of the presiding judge, the Honorable Henry Coke Morgan, Jr. ECF No. 551. The Court denied the motion and entered judgment in favor of Plaintiff Centripetal Networks, LLC (“Centripetal”). ECF Nos. 619, 621, 638. Cisco appealed. Before the appeal was decided, Judge Morgan passed away. Thereafter, the United States Court of Appeals for the Federal Circuit reversed the denial of Cisco’s recusal motion. *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 38 F.4th 1025, 1030–33 (Fed. Cir.), *cert. denied*, 143 S. Ct. 487 (2022). As a result, the Federal Circuit vacated the infringement opinion and judgment in favor of Centripetal, as well as this Court’s denial of Cisco’s motion for a new trial. *Id.* at 1040. The Federal Circuit remanded the case for “further proceedings before a newly appointed judge, who shall decide the case without regard for the vacated opinions and orders” and directed that the remand be governed by Federal Rule of Civil Procedure 63. *Id.*

Based upon review of the record and the arguments of the parties, the Court FINDS that Centripetal has failed to meet its burden to establish infringement of the ’193, ’806, or ’176 Patents.

Consistent with this determination, the Court enters the following findings of fact and conclusions of law. Fed. R. Civ. P. 52(a).<sup>1</sup> Having found that Centripetal has failed to establish infringement, the Court need not reach issues related to patent validity or damages. Finding “no just reason for delay,” the Court DIRECTS the Clerk to enter partial final judgment in favor of Cisco pursuant to Rule 54(b) of the Federal Rules of Civil Procedure.

## I. BACKGROUND

This case was brought by Centripetal Networks, Inc. against Cisco Systems, Inc. on February 13, 2018. ECF No. 1. On March 29, 2018, Centripetal filed an Amended Complaint, alleging infringement of U.S. Patent Nos. 9,560,077 (“the ’077 Patent”); 9,413,722 (“the ’722 Patent”); 9,160,713 (“the ’713 Patent”); 9,124,552 (“the ’552 Patent”); 9,565,213 (“the ’213 Patent”); 9,674,148 (“the ’148 Patent”); 9,686,193 (“the ’193 Patent”); 9,203,806 (“the ’806 Patent”); 9,137,205 (“the ’205 Patent”); 9,917,856 (“the ’856 Patent”); and 9,560,176 (“the ’176 Patent”). ECF No. 29.

Between July 12, 2018, and September 18, 2018, Cisco filed petitions for *inter partes* review (“IPR”) challenging claims asserted in nine of the eleven asserted patents and requested that the Court stay the action to allow for the resolution of the petitions by the Patent Trial and Appeal Board (“PTAB”). ECF No. 45. On February 25, 2019, the Court granted the stay. ECF No. 58. Thereafter, Centripetal moved to lift the stay, and on September 18, 2019, the Court granted

---

<sup>1</sup> While the Court has endeavored to separate factual findings from legal conclusions for each patent in the below analysis, the headings are not meant to be limiting. Findings of fact may include, apply, restate, or embody conclusions of law, and vice versa. Additionally, while the Court may cite testimony and/or documentary evidence to support a finding, this is not meant to imply that the cited evidence is the only evidentiary support for the finding. Some of the findings are based on the record or inferences from the record which are not cited. To the extent any of the proposed findings of fact or conclusions of law submitted by the parties are inconsistent with the Court’s findings and conclusions below, they are rejected.

the request in part, lifting the stay as to patents and claims not then subject to IPR proceedings. ECF No. 68 at 7.

On February 6, 2020, the Court held a *Markman* hearing in which it construed certain disputed claim terms. ECF No. 202 (“*Markman* Order”). Specifically, the Court made the following determinations:

<b>Term</b>	<b>Court’s Construction</b>
<b>Packets</b>	Plain and ordinary meaning in the context of the claim in which the term appears
<b>Preambles</b>	Limiting
<b>Configured to</b>	Plain and ordinary meaning which requires that the action actually do the function automatically
<b>Dynamic security policy</b>	A changeable set of one or more rules, messages, instructions, files, or data structures, or any combination thereof, associated with one or more packets
<b>Correlate, based on a plurality of log entries</b>	Packet correlator may compare data in one or more log entries with data in one or more other log entries
<b>Responsive to correlating</b>	Plain and ordinary meaning
<b>Generate, based on the correlating, one or more rules</b>	Plain and ordinary meaning
<b>Proxy system</b>	A proxy system which intervenes to prevent threats in communications between devices

*Markman* Order at 22.

Subsequently, Centripetal waived its right to a jury trial and consented to a bench trial. ECF No. 328 at 7:23–8:23. At the trial, Centripetal argued that Cisco infringed claims 18 and 19 of the ’193 Patent, claims 9 and 17 of the ’806 Patent, claims 11 and 21 of the ’176 Patent, claims 24 and 25 of the ’856 Patent, and claims 63 and 77 of the ’205 Patent. ECF No. 411 at 2. The 22-day bench trial and subsequent damages hearing were held virtually using the Zoom video conference platform. *See* ECF Nos. 496–550 (“Tr.”).

During the trial, Centripetal called numerous fact and expert witnesses. Centripetal's fact witnesses who provided live testimony included: Mr. Steven Rogers, Founder and CEO of Centripetal, Tr. 228:5–8; Dr. Sean Moore, the Chief Technology Officer and Vice President of Research at Centripetal and an inventor on all the asserted patents in this case, Tr. 301:21–25, 314:25–315:2; Mr. Jonathan Rogers, the Chief Operating Officer at Centripetal, Tr. 1194:10–11; and Mr. Christopher Gibbs, the Senior Vice President of Sales at Centripetal, Tr. 1296:24–1297:2. Centripetal also presented testimony from the following Cisco employees through video deposition: Mr. Saravanan Radhakrishnan, Mr. Rajagopal Venkatraman, Dr. David McGrew, Mr. Sunil Amin, and Mr. Sandeep Agrawal. Tr. 405:1–2, 407:13–14, 409:6–7, 410:15–16, 419:8–9.

Centripetal's expert witnesses who testified during its case-in-chief included: Dr. Nenad Medvidovic, an expert in computer science and computer architecture who presented a technology tutorial to the Court and also opined on the importance of the patented technology as it relates to the accused products, Tr. 18:4–16, 1144:22–1145:2; Dr. Michael Mitzenmacher, an expert in computer networking and computer security who presented an infringement opinion as to the '193, '806, and '205 Patents, Tr. 431:16–23; Dr. Eric Cole, an expert in cybersecurity and the cybersecurity industry who presented an infringement opinion as to the '856 and '176 Patents, Tr. 880:20–881:5, 886:9–11, 975:19–21; Dr. Aaron Striegel, an expert in computer networking and computer networks who opined on damages apportionment, Tr. 1337:6–14, 1337:19–23, 1340:1–6; Mr. Lance Gunderson, an expert in patent damages who opined on damages royalty rates, Tr. 1440:4–9, 1441:2–14; and Mr. James Malackowski, an expert in business and intellectual property valuation and patent licensing who opined on the valuation of the patents and future damages, Tr. 1573:14–19, 1577:4–11.

In Centripetal's rebuttal validity case, it additionally called the following expert witnesses: Dr. Alessandro Orso, an expert in computer networks and network security who provided an opinion as to the validity of the '193 and '806 Patents, Tr. 2989:12–14, 22–25; Dr. Trent Jaeger, an expert in computer and network security who provided an opinion as to the validity of the '856 and '176 Patents, Tr. 3102:5–7, 18–23; and Dr. Aaron Striegel, a computer science expert who provided an opinion as to secondary considerations of non-obviousness for the asserted patents, Tr. 3196:16–18.

Cisco likewise called numerous fact and expert witnesses. Cisco's fact witnesses who provided live testimony included: Mr. Hari Shankar, a Principal Engineer and Software Architect at Cisco responsible for the design of certain features of the accused products, Tr. 2499:15, 2500:3–5; Mr. Daniel Llewallyn, a Software Engineer for Cisco who helped develop the Stealthwatch product line, Tr. 2141:19; Mr. Peter Jones, a Distinguished Engineer in the Enterprise Network Hardware Group at Cisco, Tr. 2543:12–17; Mr. Timothy Keanini, a Distinguished Engineer at Cisco involved with Stealthwatch, Tr. 2810:4–6; Mr. Karthik Subramanian, Partner at venture capital firm Evolution Equity Partners and previous leader of Cisco's Corporate Development Team for Cybersecurity, Tr. 2827:23–25, 2828:17–18; Mr. Michael Scheck, Senior Director of Incident Command at Cisco, Tr. 1658:23–24; Dr. David McGrew, a Cisco Fellow who was responsible for leading a research and development project at Cisco relevant to the '856 Patent, Tr. 1756:23, 1759:10–12; and Mr. Matt Watchinski, a Cisco employee responsible for Cisco's threat intelligence organization, Tr. 2682:11–13. Cisco also presented testimony from current and former Centripetal employees through video deposition, including: Mr. Douglas DiSabello, Mr. Haig Colter, Dr. Sean Moore, Mr. Jess Parnell, Mr. Justin Rogers, Mr. Christopher Gibbs, and Mr.

Gregory Akers. Tr. 1800:22–23, 2139:9–10, 2575:4–5, 2709:19–20, 2711:12–13, 2722:3–4, 2723:22–23.

Cisco's expert witnesses who testified at trial included: Dr. Kevin Almeroth, an expert in computer networks and network security who presented a technology tutorial to the Court and provided an opinion as to non-infringement, invalidity, and damages for the '176 Patent, Tr. 71:14–72:1, 2212:1–3, 12–18; Dr. Mark Crovella, an expert in computer networks and network security who provided an opinion as to non-infringement, invalidity, and damages for the '193 Patent, Tr. 2349:1–24; Dr. Narasimha Reddy, an expert in computer networks and network security who provided an opinion as to non-infringement, invalidity, and damages for the '806 Patent, Tr. 2579:20–22, 2580:6–10; Dr. Douglas Schmidt, an expert in computer networks and network security who provided an opinion as to non-infringement, invalidity, and damages for the '856 Patent, Tr. 1811:18–19, 1813:4; Dr. Kevin Jeffay, an expert in computer networks and network security who provided an opinion as to non-infringement and damages for the '205 Patent, Tr. 2727:2–19; and Dr. Stephen Becker, an expert in economic damages analysis who provided an opinion as to damages, Tr. 2863:3–19.

At the close of Centripetal's case in chief, Cisco made a motion for judgment on partial findings pursuant to Fed. R. Civ. P. 52(c). ECF No. 444. The Court denied the motion. Tr. 1635:14–1656:13. After the conclusion of the trial and prior to the Court's entry of its findings of fact and conclusions of law, Cisco moved for Judge Morgan's recusal. ECF No. 557 at 3–11; *see also* 28 U.S.C. § 455(a), (b)(4). The Court denied the motion. *See* ECF No. 619. On October 5, 2020, Judge Morgan entered a decision on the merits finding that Cisco willfully infringed the asserted claims of the '806, '176, '193, and '856 Patents. ECF No. 621 at 29, 57, 72, 95, 107. The Court found the '205 Patent claims that were pursued at trial were not infringed. *Id.* at 123. Cisco subsequently

moved for a new trial pursuant to Rule 59(a)(2) of the Federal Rules of Civil Procedure. ECF No. 625.

On November 18, 2020, the Court dismissed without prejudice Centripetal's claims related to the patents that had previously been stayed due to pending IPR proceedings. ECF No. 633. This included all asserted claims related to the '213 Patent, the '552 Patent, the '713 Patent, the '148 Patent, the '077 Patent, and the '722 Patent, as well as the '205 Patent claims that were not pursued at trial. *Id.*

On March 17, 2021, Judge Morgan denied Cisco's motion for a new trial and entered final judgment in favor of Centripetal. ECF No. 638. Cisco timely appealed to the Federal Circuit. On June 23, 2022, the Federal Circuit reversed the denial of Cisco's recusal motion and, as a result, vacated the infringement opinion and judgment in favor of Centripetal, as well as the Court's denial of Cisco's motion for a new trial. *Centripetal Networks, Inc.*, 38 F.4th at 1030–33, 1040. Following Judge Morgan's passing on May 1, 2022, the Court of Appeals instructed that the case “be assigned to a new judge in the normal course, pursuant to Rule 63, which allows a replacement judge ‘if a judge conducting a hearing or trial is unable to proceed.’” *Id.* at 1039 (quoting Fed. R. Civ. P. 63). On August 23, 2022, this case was reassigned to the undersigned.

Rule 63 of the Federal Rules of Civil Procedure provides:

If a judge conducting a hearing or trial is unable to proceed, any other judge may proceed upon certifying familiarity with the record and determining that the case may be completed without prejudice to the parties. In a hearing or a nonjury trial, the successor judge must, at a party's request, recall any witness whose testimony is material and disputed and who is available to testify again without undue burden. The successor judge may also recall any other witness.

In an analogous context, the United States Court of Appeals for the Fourth Circuit recognized that “parties may consent to having the entire case decided upon the record or they may agree as to which witnesses need to testify again.” *Henry A. Knott Co. v. Chesapeake & Potomac*

*Tel. Co. of W. Va.*, 772 F.2d 78, 87 (4th Cir. 1985). Here, the parties were given the opportunity to recall any witness whose testimony was material and disputed. Neither party chose to recall any witnesses.

Cisco made two motions in connection with the Rule 63 hearing. First, Cisco moved to renew its motion to partially stay the case as to the '856 Patent, and second, it moved to supplement the trial record. ECF Nos. 687, 691. The Court granted Cisco's renewed stay motion due to the PTAB's issuance of a final written decision declaring that the '856 Patent claims asserted by Centripetal were unpatentable.<sup>2</sup> ECF No. 715; *see also* ECF No. 686. The Court also granted in part Cisco's motion to supplement the record. ECF Nos. 750, 753, 754 ("R. 63 Tr.") at 10:4–5. Specifically, the Court granted Cisco's request to admit DTX-1 and DTX-369, which were both made available to Judge Morgan in their entirety during the trial but had only been partially admitted into the record. R. 63 Tr. 10:7–22. The Court also granted the request to admit two documents that post-dated the trial—Centripetal's preliminary response regarding the '176 Patent in IPR proceedings before the PTAB, attached as Exhibit 3 to Cisco's memorandum in support of its motion, and Exhibit 4, the Patent Office's decision denying institution of *inter partes* review of the '176 Patent. R. 63 Tr. 10:23–11:5; ECF Nos. 692-4, 692-5. The Court denied Cisco's request to admit the testimony of Dr. Sean Moore, finding that it was inappropriate given that Cisco had the opportunity to call Dr. Moore to appear at the Rule 63 hearing and chose not to do so. R. 63 Tr. 11:13–22; ECF No. 692-2.

On June 21, 2023, the undersigned certified her familiarity with the record, ECF No. 742, and on June 22, 23, and 26, 2023, the Court held a hearing pursuant to Rule 63. The parties each

---

<sup>2</sup> The Court had initially denied Cisco's request for a partial stay of the case as to the '856 Patent prior to the PTAB's issuance of its final written decision. *See* ECF No. 675 at 10:6–7; ECF No. 677.



presented a technology tutorial—through Dr. Nenad Medvidovic for Centripetal and Dr. Kevin Almeroth for Cisco. *See* R. 63 Tr. 13:17–208:17. Counsel for both sides also presented argument on each of the ’193, ’806, and ’176 Patents. *See id.* at 217:25–702:2. Prior to the Rule 63 hearing, Centripetal and Cisco filed Proposed Findings of Fact and Conclusions of Law. ECF Nos. 725 (“Centripetal PFF” & “Centripetal PCL”),<sup>3</sup> 737-1 (“Cisco PFFCL”). Following the hearing, the parties submitted supplemental proposed findings regarding the post-trial prosecution history of the ’176 Patent. ECF Nos. 766, 768-1.

## II. LEGAL STANDARD

The infringement analysis is a two-step process: “[f]irst, the Court determines the scope and meaning of the patent claims asserted, and then the properly construed claims are compared to the allegedly infringing device.” *Cordis Corp. v. Bos. Sci. Corp.*, 658 F.3d 1347, 1354 (Fed. Cir. 2011) (quoting *Cybor Corp. v. FAS Techs., Inc.*, 138 F.3d 1448, 1454 (Fed. Cir. 1998) (en banc)). In order to show infringement, “the plaintiff must establish by a preponderance of the evidence that the accused device infringes one or more claims of the patent either literally or under the doctrine of equivalents.” *Bayer AG v. Elan Pharm. Rsch. Corp.*, 212 F.3d 1241, 1247 (Fed. Cir. 2000). “To prove literal infringement, the patentee must show that the accused device contains *each and every limitation* of the asserted claims.” *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1215 (Fed. Cir. 2014) (emphasis in original). “[I]f even one limitation is not met, there is no literal infringement.” *E.I. du Pont De Nemours & Co. v. Unifrax I LLC*, 921 F.3d 1060, 1073 (Fed. Cir. 2019). Additionally, “[i]f an asserted claim does not literally read on an accused product,

---

<sup>3</sup> The Court refers to Centripetal’s Proposed Findings of Fact and Conclusions of Law as “Centripetal PFF” when discussing the Proposed Findings of Fact numbered paragraphs (pp. 1–163), and “Centripetal PCL” when discussing the Proposed Conclusions of Law numbered paragraphs (pp. 163–232).

infringement may still occur under the doctrine of equivalents if there is not a substantial difference between the limitations of the claim and the accused product.” *Bayer AG*, 212 F.3d at 1250 (citing *Warner–Jenkinson Co. v. Hilton Davis Chem. Co.*, 520 U.S. 17, 29, 39–41 (1997)). This can be demonstrated “by showing on a limitation by limitation basis that the accused product performs substantially the same function in substantially the same way with substantially the same result as each claim limitation of the patented product.” *Crown Packaging Tech., Inc. v. Rexam Beverage Can Co.*, 559 F.3d 1308, 1312 (Fed. Cir. 2009) (citing *Warner–Jenkinson Co.*, 520 U.S. at 17, 39–40).

Infringement of a patent claim can be proven either directly or indirectly. To prove direct infringement, the plaintiff must show that the defendant itself “makes, uses, offers to sell, or sells any patented invention, within the United States.” 35 U.S.C. § 271(a). Indirect infringement allows a plaintiff to bring in the actions of other parties, such as the defendant’s customers, but requires the plaintiff to satisfy certain knowledge and intent requirements for the defendant. *Id.* § 271(b)–(c). Centripetal has asserted that Cisco is liable as both a direct and indirect infringer. *See* Centripetal PCL ¶¶ 4–84.

### III. TECHNOLOGY OVERVIEW

#### A. Networking and Security

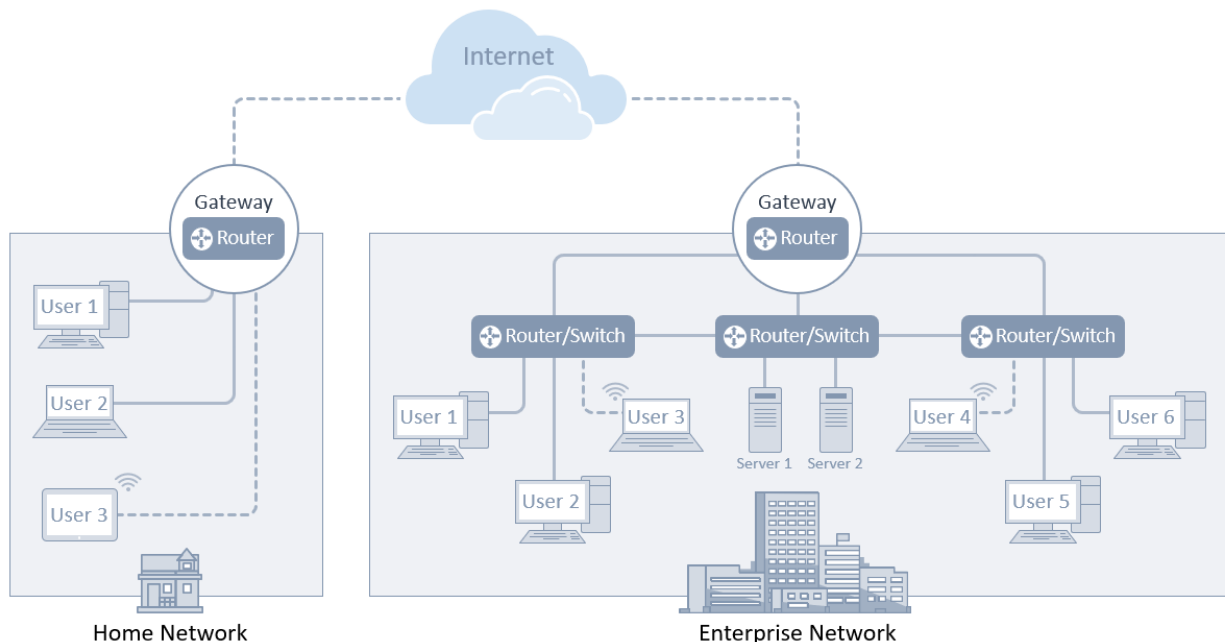
The three patents at issue in this case involve methods designed to enhance the security of computer networks. In particular, the patents involve ways in which data packets are processed as they proceed through different parts of networks.

A network is comprised of computers that are connected through routers and switches. Switches generally connect computers within an organization, and routers generally connect

computers to other computers outside of an organization. Tr. 624:12–19. The Internet is an interconnected network of networks. R. 63 Tr. 84:2–9.

Data flows through networks in the form of packets. Packets generally have two basic components—a header and a payload. R. 63 Tr. 19:23–20:9. The header contains the information that switches and routers need to deliver packets to their destination. R. 63 Tr. 86:7–10. The payload contains the underlying information that the packet is transmitting to its destination. R. 63 Tr. 20:1–4.

The diagram below depicts the general structure of two computer networks—a “Home Network” and an “Enterprise Network.” Fig. 1. The “Home Network” consists of three computers connected to a gateway router (Users 1, 2, and 3). The “Enterprise Network” consists of three sets of computers (Users 1, 2, and 3, Servers 1 and 2, and Users 4, 5, and 6) connected to three separate routers or switches, which are all connected to a single gateway router.



Cisco Demonstrative, Rule 63 Hearing.

For User 1 in the Home Network to send an email to User 6 in the Enterprise Network, a series of packets containing that email (also referred to as the packet “flow”) are forwarded from User 1 to the gateway router in the Home Network, pass through any number of other networks (depicted in the above diagram as the “Internet”), then through the gateway router of the Enterprise Network, to a final router or switch, then to User 6’s computer.

As packets are transmitted between different networks, security is a key consideration. To enhance network security, protections are implemented in firewalls<sup>4</sup> and similar appliances, as well as in routers and switches themselves. R. 63 Tr. 116:8–14, 11–16. These network devices can use certain kinds of rules (access control lists, or “ACLs”) to determine which packets are allowed to access various network resources. Tr. 537:18–21, 2550:1–4.

The patents at issue here each involve specific ways these kinds of devices process packets to enhance network security. The ’193 Patent involves a method for blocking data exfiltrations,<sup>5</sup> the ’806 Patent involves a technique for changing packet-filtering rules, and the ’176 Patent involves a process for tracing the source of packets that pass through a network device.

## **B. Centripetal’s RuleGATE Product**

Centripetal has asserted that each of the patents is practiced by Centripetal’s RuleGATE product, a packet-filtering device that was first sold in the United States in December 2014. Tr. 285:24–286:1, 1381:13–1385:19; PTX-1215 (patent-by-patent analysis). The RuleGATE product ingests data from multiple threat intelligence feeds and was marketed by Centripetal as being able to run up to 5 million different security rules on packets. PTX-550; PTX-547 at 389. The product

---

<sup>4</sup> Firewalls are specialized devices installed in the network that filter incoming and outgoing traffic to block malicious activity. R. 63 Tr. 117:11–16.

<sup>5</sup> Exfiltration involves a circumstance where an attacker gains access to a computer inside of a network and sends protected information outside of that network. R. 63 Tr. 107:5–16.

can be deployed either “inline” or “out-of-band.” Tr. 1382:12–22. Packets are processed directly through a device in an “inline” configuration, while an “out-of-band” setup indirectly monitors packets. *Id.*

### **C. Overview of Cisco’s Technology**

Centripetal’s infringement case focused on a set of updates Cisco made in 2017 to certain of its switches, routers, firewalls, and related technology. Centripetal argued that these updates implemented network security functionality into Cisco’s devices that infringes on Centripetal’s patents. Centripetal’s allegations of infringement are against combinations of Cisco hardware and software. A brief description of each of these products is provided below.

#### Catalyst 9000 Switches

Centripetal accused Cisco’s switches that are part of the Catalyst 9000 series, including the Catalyst 9300, 9400, and 9500 series running IOS-XE 16.5 and subsequent releases, as well as the Catalyst 9800 series wireless controller running IOS-XE 16.10 and subsequent releases, of infringement (the “Accused Switches”). ECF No. 408 at 17 n.3; *see also* Tr. 434:14–17. In addition to the operating system running on the switches (i.e., the software code), customers are also able to add a “software subscription referred to as Cisco [Digital Network Architecture (“DNA”) Center],” which is discussed further below. PTX-560 at 772. Cisco advertised the Accused Switches as being “built for security” and “a critical part of an end-to-end integrated security solution, one that detects and stops threats.” PTX-1260 at 849. The Accused Switches are able to enforce a variety of security rules to either forward or drop packets. Tr. 39:15–40:4, 440:8–442:25, 450:23–452:11. Centripetal argued the Accused Switches infringe the asserted claims in the ’193 Patent, the ’806 Patent (when used in combination with the DNA Center), and the ’176 Patent

(when used in combination with Stealthwatch and Cognitive Threat Analytics). Tr. 433:12–434:1 ('193 Patent); Tr. 571:17–572:3 ('806 Patent); Tr. 975:17–21, 995:19–21 ('176 Patent).

#### ISR/ASR Routers

Centripetal accused Cisco's Integrated Services Routers ("ISR") and Aggregation Services Routers ("ASR"), including the 1000 and 4000 series ISR and the 1000 series ASR routers running the IOS-XE 16.5 operating system and subsequent versions, of infringement (the "Accused Routers"). ECF No. 408 at 17 n.4; Tr. 433:24–434:1. Cisco advertised the Accused Routers as "includ[ing] integrated security, advanced analytics, automated provisioning, and application optimization, to deliver a complete solution." PTX-1226 at 638; Tr. 443:17–444:10. Similar to the Accused Switches, Centripetal alleged that the Accused Routers infringe the asserted claims of the '193 Patent, the '806 Patent (when used in combination with the DNA Center), and the '176 Patent (when used in combination with Stealthwatch and Cognitive Threat Analytics). Tr. 433:12–434:1 ('193 Patent); Tr. 571:17–572:3 ('806 Patent); Tr. 975:17–21, 995:19–21 ('176 Patent).

#### Digital Network Architecture Center

Cisco's Digital Network Architecture ("DNA") Center is a subscription service that can be used to configure and manage the Accused Switches and Routers. Tr. 55:13–21, 575:15–577:8, 579:10–580:24; PTX-560 at 772; PTX-1294 at 3. Specifically, the DNA Center manages and sends rules to the Accused Switches and Routers. Tr. 575:15–577:8; PTX-1263 at 179. As noted, Centripetal accused the DNA Center, when used in combination with the Accused Switches or Routers, of infringing the asserted claims in the '806 Patent. Tr. 571:17–572:3.

#### Stealthwatch with Cognitive Threat Analytics

Stealthwatch is a part of the DNA Center subscription that can be used with the Accused Switches and Routers. Tr. 450:23–452:11, 453:16–454:20; *see also* PTX-577 at 007; PTX-992 at

1–2. It was updated in 2017 to include Cognitive Threat Analytics. Tr. at 2148:8–11. Cisco advertised Stealthwatch with Cognitive Threat Analytics as having the ability to analyze traffic flowing from the Accused Switches and Routers to “detect and respond to threats in real-time.” PTX-482 at 664. The key components of Stealthwatch include two pieces of hardware—the Stealthwatch Flow Collector and the Stealthwatch Management Console. Tr. 2143:2–12. Cisco indicated that Cognitive Threat Analytics is a cloud-based service that is based overseas in Dublin and London. Tr. 2183:9–15; 2189:19–2190:1. As noted, Centripetal accused Stealthwatch with Cognitive Threat Analytics, when used with the Accused Switches and Routers, of infringing the asserted claims of the ’176 Patent. Tr. 975:17–21, 995:19–21.

#### Identity Services Engine

Cisco’s Identity Services Engine is software that can be used with the Accused Switches and Routers to provide “[c]entral network device management” and “granular control of who can access which network device.” PTX-411 at 891. The Identity Services Engine is responsible for “tracking [the] identity of users and user computers on a network and for setting the limits of user and computer access to other devices on the network.” Tr. 149:20–23. The parties dispute whether the Identity Services Engine is accused of infringement. *See infra* note 8. In any case, the device plays a role in the quarantine rule that Centripetal has accused of infringing the asserted ’193 Patent claims.

#### Adaptive Security Appliance and Firepower Firewalls

Centripetal also accused certain of Cisco’s firewalls, including the Adaptive Security Appliance 5500 with Firepower services (version 9.4 and later) and Cisco’s Firepower Appliance 1000, 2100, 4100, and 9300 series running Firepower Threat Defense 6.0 and later (the “Accused Firewalls”), of infringement. ECF No. 408 at 17 n.5; *see also* Centripetal PFF ¶ 78. Centripetal

argued that the Accused Firewalls, used in combination with the Firepower Management Center, infringe the asserted claims of the '806 Patent. Tr. 435:4–16, 571:17–572:3, 642:4–12.

#### Firepower Management Center

The Firepower Management Center is Cisco software that is used to manage the Accused Firewalls. Tr. 63:24–64:10, 558:1–14. It can configure and operate multiple firewall devices in the network. Tr. 558:1–14, 643:6–10. In 2017, the Threat Intelligence Director was added to the Firepower Management Center. PTX-1291 at 1, 7; Tr. 651:18–653:6. The Threat Intelligence Director receives rules from various sources and preprocesses them into rule sets that can be used by Firepower Management Center. Tr. 651:18–653:6. As noted, Centripetal accused the Firepower Management Center with the Threat Intelligence Director, in combination with the Accused Firewalls, of infringing the asserted claims of the '806 Patent. Tr. 435:4–16, 571:17–572:3, 642:4–12.

### IV. '193 PATENT

#### A. Findings of Fact

##### Asserted Claims in the '193 Patent

1. The '193 Patent was issued on June 20, 2017, and has the title “Filtering Network Data Transfers.” ECF No. 701 (“Stip.”) ¶¶ 8–9. The patent was filed on February 18, 2015, as a continuation of application No.13/795,882. Stip. ¶ 9. The patent has a priority date of March 12, 2013. Stip. ¶ 10; JTX-4 (“'193 Patent”) at 1:6–9.

2. The asserted claims are claims 18 and 19. Stip. ¶ 11. They are, respectively, a packet-filtering system claim and a computer readable media claim. *Id.* Claim 18 is laid out below:

*A system comprising:*

*at least one processor; and*



*a memory storing instructions that when executed by the at least one processor cause the system to:*

*receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;*

*responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:*

*apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and*

*drop each packet in the first portion of packets; and*

*responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:*

*apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and*

*forward each packet in the second portion of packets toward the third network.*

'193 Patent at 14:1–36.

3. Claim 19 is identical to claim 18 except that it is a computer readable media<sup>6</sup> claim.

Stip. ¶ 13. Claim 19 substitutes the introductory language of claim 18, “[a] system comprising: at least one processor; and a memory storing instructions that when executed by the at least one

---

<sup>6</sup> Computer readable media is software comprising source code that is loaded into computer hardware through a device such as a CD-ROM, memory card, or flash drive. Tr. 473:3–23. This media comprises readable instructions for the intended computer to operate. *Id.*

processor cause the system to” with “[o]ne or more non-transitory computer-readable media comprising instructions that when executed by one or more computing devices cause the one or more computing devices to.” ’193 Patent at 14:1–15:2. For all relevant purposes, the parties treat claims 18 and 19 the same. Stip. ¶ 13.

4. The ’193 Patent describes a method of filtering packets to prevent data exfiltrations. The specification explains that “[a] category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet) has proven to be especially difficult for conventional cyber defense systems to prevent.” ’193 Patent at 1:24–27. It notes that one reason for this is that “many exfiltrations are facilitated by using popular network data transfer protocols . . . that often appear to an observer (e.g., a conventional cyber defense system) as normal network behavior.” ’193 Patent at 1:27–32. One of the inventors of the ’193 Patent, Dr. Sean Moore, characterized the technology as involving the prevention of exfiltration of confidential data by cyber criminals. Tr. 343:12–16. Likewise, Centripetal’s expert witness on the ’193 Patent, Dr. Mitzenmacher, noted that the ’193 Patent claims relate to the forwarding or dropping of packets for the purpose of preventing exfiltrations. Tr. 465:16–21.

5. At a basic level, claims 18 and 19 describe a system that drops or forwards packets based on two criteria: (1) the destination of the packets and (2) the type of data transfer associated with the packets. ’193 Patent at 14:1–15:2.

6. As set forth in claim 18, the system first “receive[s] . . . a plurality of packets” from a computer in a “first network.” *Id.* at 14:5–6. Then, if the packets are “destined for [a] second network,” and the system makes a “determination that the . . . portion of packets comprises data corresponding to [rule] criteria . . . configured to prevent a particular type of data transfer from the

first network to [the] second network,” an operator is applied that is “configured to drop packets associated with the particular type of data transfer.” *Id.* at 14:9–22.

7. Alternatively, if the packets are “destined for a third network” and the system makes a “determination that the . . . packets comprise[] data that does not correspond to the [rule] criteria,” the claim states that an operator is applied that is “configured to forward packets not associated with the particular type of data transfer to the third network.” *Id.* at 14:23–36. Claim 19 describes the same technique. *See id.* at 14:41–56.

8. The patent’s specification describes this as a two-stage filtering method:

[T]he first stage may determine if the network policy allows any communications between the resources identified in the 5-tuple rule; if so, the second stage may determine if the policy allows the specific method or type of communication (e.g., file read, file write, encrypted communication, etc.) between the resources.

’193 Patent at 8:45–52. The specification further explains that this filtration method would “allow users to surf (e.g., GET) to one or more websites attached to the Internet,” but prevent riskier types of data transfers associated with exfiltration, such as “users . . . writing (e.g., PUT) data files or posting (e.g., POST) forms to one or more websites.” *Id.* at 2:43–54; *see also id.* at 7:10–20, 7:32–37. The specification distinguishes this solution from quarantining a network computer entirely, noting that “[w]hile enterprise X could simply block all communications to networks . . . it does not fully trust, this would likely result in enterprise X blocking access to most of the Internet.” *Id.* at 7:26–29.

The Accused Switches and Routers

9. Centripetal alleged that Cisco’s Accused Switches and Routers<sup>7</sup> infringe claims 18 and 19 of the ’193 Patent when the devices use specific packet-filtering rules to determine if a packet should be permitted or dropped. Centripetal PFF ¶¶ 153–60; Centripetal PCL ¶¶ 19–30; Tr. 791:14–792:24; *see also* Tr. 2377:13–2379:1. At trial, Centripetal relied on the infringement opinion of expert witness Dr. Michael Mitzenmacher and Cisco relied on the non-infringement opinion of expert witness Dr. Mark Crovella. Both parties also called a variety of fact witnesses.

10. To begin, Cisco’s Accused Switches and Routers apply packet-filtering rules to drop or forward packets that are transmitted through the devices. Tr. 488:1–489:3; PTX-1276 at 216. To do this, the devices use processors, specifically a programmable Application Specific Integrated Circuit containing a Unified Access Data Plane. Tr. 477:23–478:8; PTX-1303 at 056. The devices also contain memory that stores software instructions, which are embodied in the operating system running on the devices. Tr. 477:16–23; PTX-1303 at 056.

11. The sets of rules that the accused devices apply to packets are called access control lists, or “ACLs,” which can cause the devices to forward or drop packets based on certain criteria. Tr. 494:3–9, 496:20–498:2, 2549:15–2550:11. There are numerous types of ACL rule sets; however, Centripetal’s infringement theory focuses on a specific type, the Security Group ACL or “SGACL.” Centripetal PCL ¶ 26; Tr. 2389:1–8; *see also* PTX-1276 at 216.<sup>8</sup>

---

<sup>7</sup> The parties dispute whether Centripetal’s infringement theory also requires the involvement of the Identity Services Engine management device. *See* Cisco PFFCL ¶ 67; Centripetal PFF ¶ 129. The Court need not reach this question because it finds that the Accused Switches and Routers do not filter packets by the “particular type of data transfer” required by the claims.

<sup>8</sup> The Accused Switches and Routers apply various sets of ACL rules when a packet enters the device and when it exits the device (i.e., on ingress and egress). Cisco’s non-infringement

12. The accused devices apply SGACL rules to packets by using scalable group tags or “SGT” tags. Tr. 494:12–24, 496:19–498:2; *see also* PTX-1276 at 216. When a packet enters an Accused Switch or Router, the device checks for the existence of an SGT tag, and if it detects one, applies the corresponding SGACL rule associated with the tag. Tr. 2383:11–19; 2423:19–2424:15. These SGT tags are attached to packets transmitted from network computers to reference the security group that the computer is assigned. *See* PTX-563 at 414–15 (listing groups such as “Supplier,” “Employee,” and “Quarantine”). Each security group is assigned a different SGT tag, and all packets transmitted from a computer in a particular security group are appended with the same SGT tag. *See* Tr. 525:7–23; Tr. 2379:2–15; PTX-1276 at 211.

13. Network administrators can modify the security group of a computer through the Identity Services Engine, a separate Cisco management device. Tr. 149:16–151:4, 527:2–17, 1698:10–14; PTX-1326; PTX-1089 at 1238 (“[Identity Services Engine] Adaptive Network Control . . . is used to change the authorization state without having to modify the overall authorization policy . . .”).

14. Although Centripetal alleged that the Accused Switches and Routers infringe the asserted claims of the ’193 Patent based on the use of SGACL rules and SGT tags generally, at trial it focused only on their use in effecting a quarantine. Centripetal PFF ¶¶ 129, 143–44, 161–66. Centripetal’s expert Dr. Mitzenmacher explained that this was because the quarantine rule was a “primary exemplar” of the accused devices’ functionality. *See* Tr. 791:17–792:24; *see also* Centripetal PFF ¶¶ 144, 154–160.

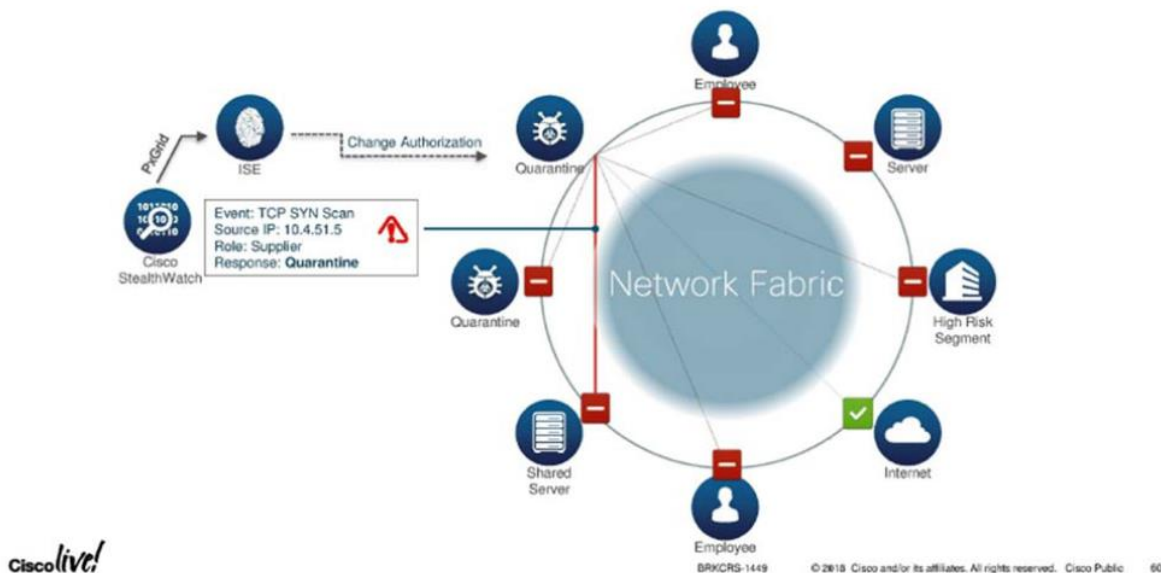
---

expert, Dr. Crovella, explained that group access control lists (“GACLs”) are applied on both ingress and egress. Tr. 2388:21–2389:19; *see also* PTX-1276 at 216. Security Group ACLs are one type of GACL. Tr. 2389:1–3.

15. The quarantine rule operates as follows: if the accused devices receive a packet containing a quarantine SGT tag, the devices apply the quarantine SGACL rule and forward or drop the packet depending on whether it is destined for a restricted destination as specified by the ACL rules. Tr. 2388:18–2389:19, 2423:19–2424:7; PTX-1276 at 216; *see also* PTX-1280 at 021; PTX-1356 at 001–005. The purpose of the quarantine rule is to limit a computer’s access to certain network destinations. *See, e.g.*, PTX-1280 at 021.

16. In other words, the quarantine rule can be set up to block a computer from accessing specific endpoints, such as part of a network containing sensitive company documents, while allowing access to other destinations, like the Internet. This is shown in the following diagram from a Cisco presentation discussed at trial:

### Rapid Threat Containment with TrustSec, ISE and Stealthwatch



PTX-563 at 415; *see also* Tr. 869:6–12.

17. Importantly, a quarantine SGT tag is attached to *all* packets transmitted from a quarantined computer. Tr. 870:15–17, 2379:2–2380:2. Additionally, the Accused Switches and

Routers only need to know the destination of a packet containing a quarantine SGT tag in order to process the packet with the quarantine SGACL rule. Tr. 869:1–12, 2377:2–10, 2385:23–2386:15, 2423:22–2424:15. Using this destination information, the Accused Switches and Routers will therefore drop *all* packets from a quarantined computer to a restricted network destination and allow *all* packets from a quarantined computer to a permitted network destination. Tr. 525:7–23, 2379:2–15, 2388:18–2389:19, 2423:19–2424:7; PTX-1276 at 216; *see also* PTX-1280 at 021; PTX-1356 at 001–005. The evidence does not show that a subset or portion of the packets—either from a quarantined computer to a restricted destination or from a quarantined computer to a permitted destination—can be dropped while other packets to that same destination are allowed.

18. This understanding was confirmed by Centripetal’s expert, Dr. Mitzenmacher, in response to a question from the Court:

**THE COURT:** Well, this this means that if your end user was, for example, a corporation and was a separate network, that you could allow some information to go to the corporation and other information not to go to them that was generated from the same source?

**WITNESS:** So the way typically the policies are instrumented is you restrict according to source and destination. So you would say, well, I’m not going to let you reach out to this other location, to this other network, right, and it will block sort of that -- it will block the communication between you and that other network.

Tr. 527:23–528:8; *see also* Tr. 869:8–12 (Dr. Mitzenmacher: “[T]he primary goal of the quarantine is to block that host from accessing certain other networks. . . . It looks at the person trying to reach out from inside and it blocks to where they can go to.”); Tr. 545:22–546:12 (Dr. Mitzenmacher: “[I]f it’s trying to go to one of these bad places, it’s going to get dropped, and if it’s going to a good place or a place that’s not one of the bad places, it will be okay.”); Tr. 2387:2–3 (Cisco expert Dr. Crovella: “The quarantine rule doesn’t do any check to see what kind of data transfer is contained in the packet.”); PTX-1280 at 021.

## B. Conclusions of Law

Centripetal has not met its burden to establish infringement of the '193 Patent because it has failed to show by a preponderance of the evidence that Cisco's technology performs each of the limitations in the patent claims. In particular, Centripetal has failed to establish that Cisco's routers and switches drop or forward packets based on the "particular type of data transfer." '193 Patent at 14:9–22, 14:27–36, 14:44–56, 14:60–15:2.

In relevant part, the claims indicate that if packets received by the system are "destined for [a] second network" and those packets meet rule criteria "configured to prevent a particular type of data transfer from the first network to [the] second network," an operator is applied that is "configured to drop [those] packets associated with the particular type of data transfer." '193 Patent at 14:9–22. The claims likewise specify that if packets are "destined for [a] third network" and "comprise[] data that does not correspond to the [type of data transfer] criteria," an operator is applied that is "configured to forward [those] packets not associated with the particular type of data transfer toward the third network." *Id.* at 14:22–36.

The disagreement between the parties comes down to whether the "particular type of data transfer" claim limitation requires a system to drop some, but not all, packets sent between two different network destinations. The evidence is overwhelming that this functionality is not present in the accused technology. *See supra* ¶¶ 15–18. Because the Court finds that the asserted claims of the '193 Patent require this functionality—filtration of a subset of packets sent between computers in two different networks—Centripetal fails to prove infringement of the '193 Patent claims. The language of the claim limitation, the patent specification, and Centripetal's statements to the PTAB all support the Court's understanding of this claim requirement. *See N. Am. Container, Inc. v. Plastipak Packaging, Inc.*, 415 F.3d 1335, 1344 (Fed. Cir. 2005) (explaining that the infringement



analysis begins by determining “the scope and meaning of the patent claims asserted” (quoting *Cybor Corp.*, 138 F.3d at 1454)).

The claim language is instructive. In order for the system to drop packets, two conditions must be met: (1) the packets from a device in a first network must be “destined for [a] second network” and (2) the packets must meet rule criteria “configured to prevent a particular type of data transfer from the first network to [the] second network.” ’193 Patent at 14:9–16. To give effect to both of these conditions, it is necessarily the case that only a portion of the packets destined for the second network meet the type of data transfer rule criteria specified by the second condition. Otherwise, the second condition would be rendered superfluous. *See W.L. Gore & Assocs., Inc. v. Medtronic, Inc.*, 834 F. Supp. 2d 465, 477 (E.D. Va. 2011) (“Claim differentiation creates a presumption that the difference between claim language is significant and that the Court should not construe terms in such a way as to render the language of a claim superfluous.”), *aff’d*, 530 F. App’x 939 (Fed. Cir. 2013).

The patent’s specification confirms the Court’s reading. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (“[T]he descriptive part of the specification aids in ascertaining the scope and meaning of the claims inasmuch as the words of the claims must be based on the description. The specification is, thus, the primary basis for construing the claims.” (quoting *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 452 (Fed. Cir. 1985))). The specification discusses functionality that would prevent users communicating with a computer in a network from conducting certain types of data transfers (e.g., risky transfers associated with exfiltration) without blocking a user’s access to that destination entirely. The specification provides the example of “allow[ing] users to surf (e.g., GET) to one or more websites attached to the Internet, . . . [while] prevent[ing] such user(s) from . . . writing (e.g., PUT) data files or posting (e.g., POST) forms.”

'193 Patent at 2:46–49. The specification notes that administrators could use this functionality “to prevent . . . exfiltrations (e.g., file transfers containing sensitive information, posting of login credentials[,] . . . etc.) to network nodes (e.g., web sites) that they may not trust.” *Id.* at 2:50–54. In other words, the patent is not designed to block all transfers between a computer and certain network destinations (like Cisco’s accused technology does), but instead allows an administrator to permit low-risk types of communication between computers in different networks, while blocking high-risk types of communication.

Finally, Centripetal’s statements to the PTAB are consistent with the Court’s interpretation. When Centripetal defended the validity of its patent before the PTAB, it distinguished the claims from prior art by emphasizing the second condition, i.e., filtration by “particular type of data transfer.” Centripetal stated that “[t]his two-stage process is reflected in each independent claim,” which includes “claims . . . 18[] and 19.” DTX-369 at 011, 018. Regarding the “second stage,” Centripetal quoted the portion of the '193 Patent’s specification that explained “the second stage may determine if the policy allows the specific method or type of communication (e.g., file read, file write, encrypted communication, etc.) between the resources.” *Id.* at 017 (quoting '193 Patent at 8:48–51); *see also Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1362 (Fed. Cir. 2017) (stating that a patent holder’s statements before the PTAB can be considered for claim construction).

Centripetal’s contrary interpretation of the claim limitation at the Rule 63 hearing—namely, that a “particular type of data transfer” refers to the *network* associated with the data transfer—is unavailing. Centripetal argued that Cisco’s Accused Switches and Routers “prevent[] particular types of data transfers to or from potentially compromised computers—*e.g.*, transfers involving networks with sensitive information—but allow transfers involving other networks, such

as the Internet.” ECF No. 703 at 10. More specifically, Centripetal has asserted that the “particular type of data transfer that is being prevented is packets that contain SGT tags that specify what network that packet can go to.” R. 63 Tr. 238:5–7.

This construction is impermissible because it reads out relevant claim language. Recall that in order to drop a packet, the claims require two conditions to be met: (1) the packets from the first network must be “destined for [a] second network” and (2) the packets must meet rule criteria “configured to prevent a particular type of data transfer from the first network to [the] second network.” Patent ’193 at 14:9–16. The claim language refers to the “particular type of data transfer” as a kind of data transfer between the first network and a second network. However, in Centripetal’s construction, the “particular type of data transfer” would encompass *all* data transfers between the first network and the second network. *See, e.g.*, R. 63 Tr. 260:5–9 (“[T]he type of data transfer from that network to another network is going to be one type. If I have a data transfer from a network to a third network, I think that is a different type of data transfer . . .”). This construction would render the check for a particular type of data transfer unnecessary, as the claims already require the system to check that the packets are destined for the second network in the first step. *See Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1369–70 (Fed. Cir. 2007) (discussing the doctrine of claim differentiation). As a result, the Court rejects Centripetal’s construction.

At times, Centripetal has also appeared to put forward a different construction, namely that a “particular type of data transfer” refers to the kind of communications contained in the transfer, but that the claim language does not require the system to drop *only* those particular data transfers. *See, e.g.*, Tr. 3281:13–3282:2. Centripetal elicited testimony at trial that suggested the claim requirements could be satisfied by a system that first detects a “particular type of data transfer” to

a specific network (such as an HTTP POST command indicative of exfiltration) and then uses that information to block all future traffic to that destination. *See, e.g.*, 787:8–13 (Dr. Mitzenmacher: “The particular type of data transfer you’re trying to stop is the exfiltration . . . And the way that was detected, right – one of the ways that can be detected is that you notice certain types of HTTP POST or HTTP GET commands.”); *see also* Tr. 512:20–513:2, 517:25–518:7, 786:5–24; Centripetal PFF ¶ 160 (“[The Accused Switches and Routers] are designed to implement quarantine rules based on detecting abnormal behavior in a variety of data transfer types, including Hypertext Transfer Protocol (HTTP), HTTP GET, and HTTP POST.”).

This second construction similarly reads out the second claim limitation that the packets meet rule criteria “configured to prevent a particular type of data transfer from the first network to [the] second network.” *See* Patent ’193 at 14:9–14. Just as in the analysis above, if the quarantine rule blocks *all* packets traveling to the second network, this necessarily means that no further determination is necessary beyond checking where the packets are headed. The fact that a rule blocking all packets to the second network may have been based on an earlier detection of abnormal traffic to that network is immaterial.<sup>9</sup> As such, the Court rejects this construction.

For the reasons stated above, the claim language, the patent’s specification, and Centripetal’s statements to the PTAB all support the Court’s conclusion that “particular type of data transfer” refers to a subset of transfers between computers in two different networks. Because

---

<sup>9</sup> The Court recognizes that it is possible to describe a quarantine rule that blocks all transfers between two networks as one “configured to prevent a particular type of data transfer,” in the same way that revoking an individual’s driving privileges obviously prevents that person from driving on a particular road. In other words, under this construction, “particular type” means “all types.” However, this is an unnatural reading that is undercut by the language of the patent specification discussing filtration of only a subset of data transfers between network destinations. *See* ’193 Patent at 2:46–50 (describing functionality “allow[ing] users to surf (e.g., GET) to one or more websites attached to the Internet, . . . [while] prevent[ing] such user(s) from . . . writing (e.g., PUT) data files or posting (e.g., POST) forms”).

the Court finds that Cisco’s quarantine rule does not have this functionality, the Accused Switches and Routers do not “determin[e] that . . . packets comprise[] data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer” or “drop packets associated with the particular type of data transfer.” ’193 Patent at 14:9–12, 18–20.<sup>10</sup>

Accordingly, the Court FINDS that Cisco’s Accused Switches and Routers do not literally infringe claims 18 or 19 of the ’193 Patent.

### **C. Doctrine of Equivalents**

Centripetal argued under the doctrine of equivalents that the Accused Switches and Routers “perform substantially the same function in substantially the same way” to achieve the same result outlined in the claims “because the collection of packets is dropped based on the corresponding rule and operator.” Centripetal PFF ¶ 176. In its literal infringement analysis, the Court found that Cisco’s technology does not meet the “particular type of data transfer” limitation because the evidence does not show that the quarantine rule is able to block a subset of the packets transferred between computers in two different networks, as the claims require. This analysis is no different when viewed under the doctrine of equivalents. The patented filtration technique is not literally present in Cisco’s technology, and Centripetal likewise does not show that a substantially similar function is performed by the accused devices. For this reason, the Accused Switches and Routers do not perform the substantially the same function or achieve the same result. Therefore, the Court FINDS that Centripetal has not met its burden of proof to show infringement of claims 18 or 19

---

<sup>10</sup> To the extent Centripetal has accused the operation of SGT tags and corresponding SGACL rules that do not involve a quarantine, the Court notes that Centripetal only presented evidence as it relates to a quarantine. While it is, of course, possible that non-quarantine SGT tags operate in a different manner than quarantine SGT tags, Centripetal has not presented any evidence of this. It would also appear that Centripetal does not believe there are material differences given its choice to present testimony of the quarantine rule as the “exemplar” for its infringement theory. *See* Tr. 791:17–792:24.

under the doctrine of equivalents. *See VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1322–23 (Fed. Cir. 2014) (discussing the requirements for finding infringement under the doctrine of equivalents).

## V. '806 PATENT

### A. Findings of Fact

#### Asserted Claims in the '806 Patent

19. The '806 Patent was issued on December 1, 2015, and has the title “Rule Swapping in a Packet Network.” Stip. ¶¶ 14–15. The patent was filed on January 11, 2013, which is the patent’s priority date. *Id.* ¶¶ 15–16.

20. The asserted claims are claims 9 and 17. *Id.* ¶ 17. They are, respectively, a packet-filtering system claim and a computer readable media claim. *Id.* Claim 9 is laid out below:

*A system comprising:*

*a plurality of processors; and*

*a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to:*

*receive a first rule set and a second rule set;*

*preprocess the first rule set and the second rule set to optimize performance of the system for processing packets in accordance with at least one of the first rule set or the second rule set;*

*configure at least two processors of the plurality of processors to process packets in accordance with the first rule set;*

*after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets;*

*process, in accordance with the first rule set, a portion of the plurality of packets;*

*signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and*

*configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set:*

*cease processing of one or more packets;*

*cache the one or more packets;*

*reconfigure to process packets in accordance with the second rule set;*

*signal completion of reconfiguration to process packets in accordance with the second rule set; and*

*responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.*

JTX-2 (“’806 Patent”) at 11:16–53.

21. Claim 9 is identical to claim 17 in every respect except that claim 17 is a computer readable media claim. Stip. ¶ 19. Claim 17 substitutes the introductory language of claim 9, replacing “[a] system comprising: a plurality of processors; and a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to” with “[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to.” ’806 Patent at 11:16–21, 12:32–34. For all relevant purposes, the parties treat claims 9 and 17 the same. Stip. ¶ 19.

22. The ’806 Patent describes a method for network protection devices to swap different sets of rules applied to packets passing through the devices. The specification notes that “[n]etwork protection devices may require time to switch between different rule sets[,] [and] [a]s rule sets increase in complexity, the time required for switching between them presents obstacles for effective implementation.” ’806 Patent at 1:20–22. It identifies two specific problems: (1) “a network protection device may be unable to process network traffic while switching between rule

sets,” and (2) “while implementing a new rule set, a network protection device may continue processing packets in accordance with an outdated rule set.” *Id.* at 1:22–28. The specification explains that “[i]n certain circumstances (e.g., in the event of a network attack), such processing [with an outdated rule set] may exacerbate rather than mitigate the impetus for the rule set switch (e.g., the effect of the network attack).” *Id.* at 1:28–31.

23. Claims 9 and 17 describe a rule swapping technique responsive to these concerns. Claim 9 provides that based on “instructions . . . executed by at least one processor,” the system “receive[s] a first rule set and a second rule set,” “preprocess[es]” both rule sets, and “configure[s] at least two processors . . . to process packets in accordance with the first rule set.” ’806 Patent at 11:18–29. Then, the system “receive[s] . . . packets” and “process[es], in accordance with the first rule set, a portion of the . . . packets.” *Id.* at 11:29–35. Next, in order to effectuate the rule swap, the system “signal[s] each processor . . . to process packets in accordance with the second rule set,” and “responsive to being signaled,” “configure[s] each processor” to take a series of actions. *Id.* at 11:35–53. Specifically, the processors are configured to “cease processing of one or more packets,” “cache the one or more packets,” and the system “reconfigure[s] [the processor] to process packets in accordance with the second rule set.” *Id.* Once reconfiguration is complete, the system “signal[s] completion of reconfiguration,” and “responsive to receiving signaling,” “process[es], in accordance with the second rule set, the one or more [cached] packets.” *Id.* at 11:45–53. Claim 17 describes the same technique. *Id.* at 12:32–64.

#### The Accused Switches, Routers, and DNA Center

24. Centripetal accused two combinations of Cisco products of infringing claims 9 and 17 of the ’806 Patent. At trial, Centripetal relied on the infringement opinion of expert witness Dr.



Michael Mitzenmacher and Cisco relied on the non-infringement opinion of expert witness Dr. Narasimha Reddy. Both parties also called a variety of fact witnesses.

25. The first accused combination is the Accused Switches and Routers combined with Cisco's DNA Center. Tr. 571:19–25; Centripetal PFF ¶ 227. Specifically, Centripetal accused these technologies of infringing the asserted claims when the switches and routers use a particular method of updating packet-filtering rules called the "FED 2.0 Hitless ACL Update." Centripetal PFF ¶ 247; *see also* Tr. 2550:18–25.

26. The Accused Switches and Routers apply sets of rules (ACLs) to packets received by the devices that cause the packets to be dropped or forwarded. Tr. 2550:1–7. The devices can receive these rule sets from a variety of sources, including the DNA Center. Tr. 2571:12–17.

27. When the switches and routers receive a new set of rules, the devices may swap out the old rules using the Hitless ACL update technique. Tr. 2550:18–2551:12. This rule update technique is also referred to as the "Hitless TCAM update." Tr. 2552:13–17; PTX 1303 at 073. According to Cisco engineer Peter Jones, this technique "refers to the ability to have a new or updated set of ACL[s] applied to a given string of packets without disabling packet processing while that change is made." Tr. 2550:23–25. He explained that, "[u]sing the Hitless update, while preparing the updated rule set for the system [the devices] continue[] to process packets with the old rule set." Tr. 2552:20–23; *see also* Tr. 2571:22–2572:1.<sup>11</sup>

28. Then, once the new rules are successfully programmed, the rules are swapped, and the Accused Switches and Routers start processing packets from that point forward with the new

---

<sup>11</sup> The Hitless ACL update replaced a prior rule swap technique used by Cisco's switches and routers that involved processing packets using a new rule set before it was fully programmed into the accused devices' software. Tr. 2552:18–23; PTX-1195 at 003, 005. This resulted in packets being discarded during the swap process. Tr. 2552:20–23; PTX-1195 at 003.

rule set. Tr. 2552:23–25, 2572:2–20. This swap happens during the devices’ existing idle period between the processing of individual packets. Tr. 2554:20–24 (Cisco engineer Peter Jones explaining that the swap occurs during the “two or four internal clock periods” between packet processing); Tr. 2619:21–25 (Cisco expert Dr. Reddy explaining that these clock periods are typically “less than a billionth of a second”). This fixed time pipeline is not affected by the rule swap; the packets continue to be processed normally regardless of whether a rule swap is occurring. Tr. 2550:12–2551:12, 2554:22–24.

29. During packet processing, packets pass through buffers in the Accused Switches and Routers. Tr. 623:18–22, 626:25–627:4, 2563:14–19; DTX-562 at 043. A packet buffer is “a piece of memory to store the contents of a packet.” Tr. 2523:10–11; *see also* Tr. 628:7–13 (Dr. Mitzenmacher explaining that “a buffer generally refers to something that you . . . leave data waiting [in] for a short period of time, until you’re ready for it”). Storing packets in a packet buffer is “a function of any . . . network interface.” PTX-1917 (Cisco engineer Martin Hughes); *see also* DTX-1688 at 166:21–168:10. In the Accused Switches, packets waiting to be processed are stored in a part of the device called the “Packet Buffers Complex.” Tr. 2563:22–2564:12; DTX-562 at 043. The Accused Routers have a similar buffer called the “Dispatcher Packet Buffer.” Tr. 623:18–22. Packets are stored in these buffers in the normal course of packet processing as well as during a rule swap. Tr. 623:18–22, 2563:7–19, 2565:11–18; PTX-1313 at 062.

#### The Accused Firewalls and the Firepower Management Center

30. Centripetal also accused a second combination of Cisco products of infringing claims 9 and 17 of the ’806 Patent: the Accused Firewalls combined with the Firepower Management Center. Tr. 435:4–16, 571:15–572:3, 642:4–12. Centripetal accused these technologies of infringing the asserted claims when the firewalls use a specific method of updating

packet-filtering rules called the “Transactional Commit Model.” Tr. 680:8–681:6; *see also* Centripetal PFF ¶¶ 291, 293.

31. The Accused Firewalls can apply sets of rules (ACLs) to packets received by the devices that cause the packets to be dropped or forwarded. Tr. 647:17–21. The firewalls can receive these rules from the Threat Intelligence Director, which is integrated into the Firepower Management Center. Tr. 648:24–649:5; *see also* Tr. 651:20–11.

32. Centripetal alleged that when the Accused Firewalls receive a new set of rules from the Threat Intelligence Director, the devices may swap out the old rules using the Transactional Commit Model.<sup>12</sup> *See* Centripetal PFF ¶ 291.

33. Using this technique, Cisco engineer Hari Shankar explained that when an Accused Firewall receives a new rule set, the rules must first be programmed into the firewall’s software.

---

<sup>12</sup> Cisco has disputed that the Accused Firewalls operate in this manner. As to the first Accused Firewall, the Firepower Appliance running Firepower Threat Defense software, Cisco engineer Hari Shankar testified that the Firepower Threat Defense software does not include the accused Transactional Commit Model feature. Tr. 2515:5–12; *see also* Tr. 2612:21–23, 2642:20–23 (Cisco expert Dr. Reddy stating that the Transactional Commit Model is not used in the Firepower appliance). Therefore, Cisco argued Centripetal’s infringement theory is untenable as to this Accused Firewall. *See* Cisco PFFCL ¶ 210. The second Accused Firewall is the Adaptive Security Appliance with Firepower Services. Tr. 571:25–572:3, 2583:16–2584:11. This firewall, Mr. Shankar noted, is actually two separately managed software firewalls “bolted together” on the same hardware, and only one of those two firewalls (the Adaptive Security Appliance software), has the accused Transactional Commit Model feature. Tr. 2504:17–25, 2514:10–21, 2612:24–2613:1; *see also* PFFCL ¶ 211. Cisco argued that this is fatal to Centripetal’s infringement theory because the Adaptive Security Appliance software receives rule updates from a non-accused management device, the Adaptive Security Device Manager. Cisco PFFCL ¶ 211–12; Tr. 2511:21–2513:3, 2612:21–2613:1. However, because the Court finds that Centripetal failed to prove infringement even if the Accused Firewalls process rule updates from the Firepower Management Center using the Transactional Commit Model, it need not resolve this dispute.

Tr. 2516:5–15. During this time, the firewall continues to process packets using the old rule set.  
Tr. 2516:11–21.<sup>13</sup>

34. Then, once programming is complete, Mr. Shankar testified that the firewalls “switch[] a mode so that any subsequent lookups will actually start using the new rule set instead of the old one.” Tr. 2517:11–13. This switch occurs during the time between the firewall’s processing of individual packets. Tr. 2521:6–12 (Mr. Shankar explaining that the “[t]he last packet that came before the programming is complete” is processed under “the old rule set,” and “[t]he next packet” is processed under “the new rule set”). Packet processing time is not changed as a result of the rule change execution. Tr. 2522:8–15.

35. Mr. Shankar explained that it was acceptable for a firewall to use an old rule set while it was programming the new rule set because it typically takes a human hours to actually create the firewall rules. Tr. 2518:22–2519:7. Therefore, he did not view the “extra few minutes for the firewall to fully program” the new rules to be an issue. *Id.*; *see also* PTX-1196 at 007 (“[I]t is acceptable to have [a] reasonable amount of delay for the new rules to take effect.”).

36. Like the Accused Switches and Routers, the Accused Firewalls use buffers when processing packets. Centripetal’s expert Dr. Mitzenmacher explained that packets are stored in a “packet buffer cache” while “waiting for the system to be ready to process them.” Tr. 707:17–20, 712:17–20. Specifically, he indicated that the firewall buffer was referred to as a “receive ring” in

---

<sup>13</sup> Similar to the Hitless ACL update, the Transactional Commit Model replaced an earlier rule swap technique in which a new rule set was applied before compilation was completed. Tr. 689:4–690:7. As noted in Cisco documentation, “[w]ith the legacy model, rule updates take effect immediately but rule matching slows down during the rule compilation period.” PTX-1241 at 253. In contrast, when the Transactional Commit Model feature is enabled, “a rule update is applied after the rule compilation is completed; without affecting the rule matching performance . . . [and] [t]his feature is useful to prevent potential packet drops during [a] large compilation of rules under high traffic conditions.” *Id.* at 253–54.

Cisco's documentation. Tr. 708:11–18; PTX-1277 at 012. Cisco engineer Mr. Shankar explained that this buffer is used during normal packet processing as well as during rule swaps. Tr. 2524:17–2525:11. Likewise, Mr. Shankar testified that the packet buffer in the Accused Firewalls operates “independent of whether rules are getting updated.” Tr. 2525:7–8, 13–17. He specifically noted that packets are not placed in a buffer in response to an update to a rule set. Tr. 2525:18–20.

## **B. Conclusions of Law**

Centripetal has not met its burden to establish infringement of the '806 Patent because it has failed to show by a preponderance of the evidence that Cisco's technology performs each of the limitations in the claims. In relevant part, the claims indicate that, in order to effectuate a rule swap, the system “signal[s] each processor . . . to process packets in accordance with the second rule set,” and “responsive to being signaled,” “configure[s] each processor” to, among other things, “cease processing of one or more packets” and “cache the one or more packets.” '806 Patent at 11:35–53. As to these claim elements, Centripetal fails to establish that, *responsive to* a signal to process packets in accordance with a second rule set, Cisco's Accused Switches, Routers, or Firewalls *cease processing* packets or *cache* those packets.

As an initial matter, the evidence shows that the Accused Switches, Routers, and Firewalls all cease processing packets, albeit very briefly,<sup>14</sup> and use a form of a queue or buffer to store packets prior to processing. *See supra* ¶¶ 27–29, 33–36. Assuming the use of a packet buffer

---

<sup>14</sup> Cisco takes some issue with this characterization, noting that “describing the interval that occurs during a normal cadence as a ‘ceasing’ of processing makes no more sense than saying someone’s heart ‘ceases’ beating when it is between two normal beats, or that the beat of a song ‘ceases’ between the regular hits on the drum.” Cisco PFFCL ¶ 169.

satisfies the claim requirement to “cache” packets,<sup>15</sup> Centripetal still fails to show that the ceasing or purported caching are taken “responsive to being signaled to process packets in accordance with the second rule set.” ’806 Patent at 11:39–42.

Centripetal’s expert at trial, Dr. Mitzenmacher, did not clearly offer an opinion as to this causal relationship. At various points, he described the ceasing and caching of packets as occurring *during* a rule swap, rather than because of it. *See, e.g.*, Tr. 627:19–25 (in reference to the Accused Routers, using Cisco engineer Martin Hughes’ testimony: “[T]he point is you need to have the packets saved while this processing switch occurs, while you’re switching the rules, and this testimony [of Mr. Hughes] verifies that the router product ha[s] a buffer and will store the packets in the buffer while they’re awaiting for processing.”); Tr. 601:23–25 (in reference to the Accused Switches, describing a “cache that hold[s] the actual packets while they’re waiting”); Tr. 707:11–12, 19–20 (in reference to the Accused Firewalls, identifying memory in the products and testifying, “[t]hat’s what stores packets before while they’re waiting for service,” and noting that “RAM is holding the packets while it’s waiting for the system to be ready to process them”).

The fact that two actions may occur at the same time or in succession, of course, does not show that one is taken “responsive to” the other. Cisco’s engineers explained that the cease/cache functionality described by Dr. Mitzenmacher occurred as a part of normal packet processing in

---

<sup>15</sup> There is some dispute as to whether a packet buffer is the same as the “cache” described in the claim language. Dr. Mitzenmacher treated the terms the same when offering his infringement opinion. *See* Tr. 628:7–13 (“So both ‘cache’ and ‘buffer’ are ways that are used by computer scientists to talk about -- they’re terms that really just mean memory.”). However, Dr. Sean Moore, one of the ’806 Patent’s inventors, distinguished between the two terms when discussing functionality covered by the patent. DTX-1688 at 167:21–168:1 (“[C]aching would be used in this sense, in this context, for, oh, those packets that you are currently processing through the old policy, you don’t want to like put those back on the buffer from whence you extracted them in the first place.”). Since the Court finds that Centripetal has failed to establish infringement on the basis that the accused devices cease processing or cache packets responsive to a rule change signal, it need not reach this argument.

Cisco's accused devices, not in response to a signal to swap to a new rule set. As to the Accused Switches and Routers, Cisco engineer Peter Jones noted that the devices swap between an old and a new rule set during the existing "two or four internal clock periods" between packet processing. Tr. 2554:20–24. Mr. Jones also testified that while all packets are held in a packet buffer to await processing in the ordinary course, this buffer has no relationship to the accused Hitless ACL rule swap technique. Tr. 2563:10–19. He explained that packet buffering in the Accused Switches operates the same way for all packets and regardless of whether the device is conducting a rule swap. Tr. 2563:7–19. Similar testimony was provided by Cisco engineer Hari Shankar with respect to the Accused Firewalls and the Transactional Commit Model update technique. Tr. 2521:6–12, 2525:2–8, 13–17. Therefore, while there is temporal relationship between a rule swap and the ceasing processing of packets, this evidence shows that there is not a causal relationship.

Centripetal responded to Cisco's argument by emphasizing that the new rule update techniques were designed to avoid dropping packets. Centripetal PCL ¶ 39 ("Cisco has implemented this new rule swap functionality in conjunction with the normal processing functionality to greatly improve the security functionality of its products without dropping packets."). Dr. Mitzenmacher explained that the inclusion of this feature indicated to him that the accused devices would need to cease processing packets during a rule swap. Tr. 634:7–14 ("[A]t the end, you update these rules, and because you're not dropping packets or somehow avoiding -- having packets avoid the rules during this transition, that also tells me that there's a signaling process that says, hey, we stop with the first rule set; we're starting to put in the second rule set."); Tr. 706:3–5 ("[W]hat you're doing is saying that I'm not going to have a period where I'm going to drop the packets."). Dr. Mitzenmacher also drew a connection between the lack of packet drops and the devices' use of a packet buffer during a rule swap. Tr. 641:18–24 ("The switches and

routers use a first rule set until an update arrives, and when the update arrives, then they use this update operation to perform the swap, as mentioned, without dropping any packets using the cache -- and, again, it's a packet buffer or cache -- and after the rule set is swapped, then you begin processing with the second rule set, as according to the claim."); *see also* Tr. 712:17–23 (“[T]he reason that [the Accused Firewalls] don’t drop any packets during the time period they’re doing the swap is because they’re using this packet buffer cache.”); PTX-1196 at 007.

The flaw in Centripetal’s no-dropped-packets argument, however, is that it does not refute Cisco’s explanation and show *causation* between a signal in the accused devices to swap to a new rule set and the ceasing and caching operations. As discussed, Cisco’s engineers testified that, as to the accused devices: (1) there is an existing idle period between the processing of each packet and (2) packets are stored in a buffer before processing. *See supra* ¶¶ 27–29, 33–36. Even though a rule swap technique might be able to take advantage of this existing functionality to avoid dropped packets, this does not mean that the ceasing and caching operations are done “responsive to” the rule swap.

Dr. Mitzenmacher’s discussion of the accused devices’ capability to cache packets does not change this analysis. In his direct testimony on the “cease” and “cache” elements, Dr. Mitzenmacher relied on diagrams showing the *normal* packet-processing architecture inside each of the accused devices. *See* PTX-1390 at 029 (Accused Switches); PTX-1313 at 062 (Accused Routers); PTX-1277 at 007 (Accused Firewalls). With respect to each diagram, he indicated that there is a portion of the processor where packets are stored, i.e., the packet buffer. *See, e.g.*, Tr. 621:21–22 (“It’s a holding place for information.”); *see also* PTX-1917. While this may show that the devices “hold the data while you’re doing the swap-over,” Tr. 621:23–24, it does not establish



causation; because the buffers are part of normal packet processing, they “hold the data” regardless of whether a swap is occurring.

Further, Centripetal’s attempt to characterize the testimony of Cisco engineer Mr. Jones as supporting its infringement position is unavailing. Centripetal argued that “[d]uring cross-examination, Mr. Jones admitted that the Catalyst 9000 Switch infringed every element . . . of the ’193 Patent[’s]” asserted claims. Centripetal PFF ¶ 236. The relevant portion of the cross examination is copied below:

Q: Now, once the compilation is complete, a signal is sent to the processor to stop processing packets with the old rule set and to start processing packets with the new rule set; isn’t that right?

A: That is correct.

Q: And then during the two to four clock periods that you mentioned yesterday, when there’s no processing of packets, the rules are swapped; isn’t that right?

A: That is correct. There is -- the processing of packets continues. Packets are processed at a maximum frequency of two to four clock periods. So we don’t stop processing the packets, there’s just an idle period between two packets.

Q: But there’s a signal that’s sent to say, stop processing packets with the old rule set and start processing packets with the new rule set, correct?

A: Yes, we swap from the old to the new.

Q: And you do that swap in between -- in that two to four clock cycles that you mentioned yesterday; correct?

A: Right.

Tr: 2572:2–20.

At the Rule 63 hearing, Centripetal argued that Mr. Jones’s agreement that “there’s a signal that’s sent to say, stop processing packets with the old rule set and start processing packets with the new rule set” indicates that the Accused Switches cease processing responsive to a signal to swap to a new rule set. *See* R. 63 Tr. 345:16–347:1. However, Mr. Jones’s statement can only be

interpreted to mean that the signal is sent “to stop processing packets with the old rule set,” not to stop the processing of those packets entirely, as the claims require. The distinction is important, as an instruction to stop processing packets in one way (with the old set) and to start processing the packets in another way (with the new set) does not require that the device cease processing the packets entirely in response to the instruction. Instead, as Mr. Jones explained, the swap occurs during the existing idle period between individual packet processing, i.e., the “two to four clock cycles” referenced above. *See* Tr. 2554:20–24. As such, Mr. Jones did not admit that the Catalyst 9000 Switch infringed the cease processing element of the asserted ’193 Patent claims.

To the extent Centripetal’s position is that the cease processing limitation can be met by a signal to stop processing packets in a certain way (i.e., to “stop processing packets with the old rule set”), the Court rejects this interpretation of the claim requirements. *See, e.g.*, R. 63 Tr. 353:21–22 (Centripetal’s counsel explaining that their argument is that “[c]ease processing of the packets means you stop processing the packets with the first rule set”). As Cisco pointed out, Centripetal’s argument improperly adds language to the claim, converting the claim requirement that the system “cease processing of one or more packets” in response to a signal to switch to a new rule set, to a requirement that it merely “cease processing of one or more packets *with the old rule set*” in response to the rule swap signal. Cisco PFFCL ¶ 172. Figure 4 in the patent specification makes clear that the claim requirement refers to ceasing processing of the packets altogether, not just with the old rule set:

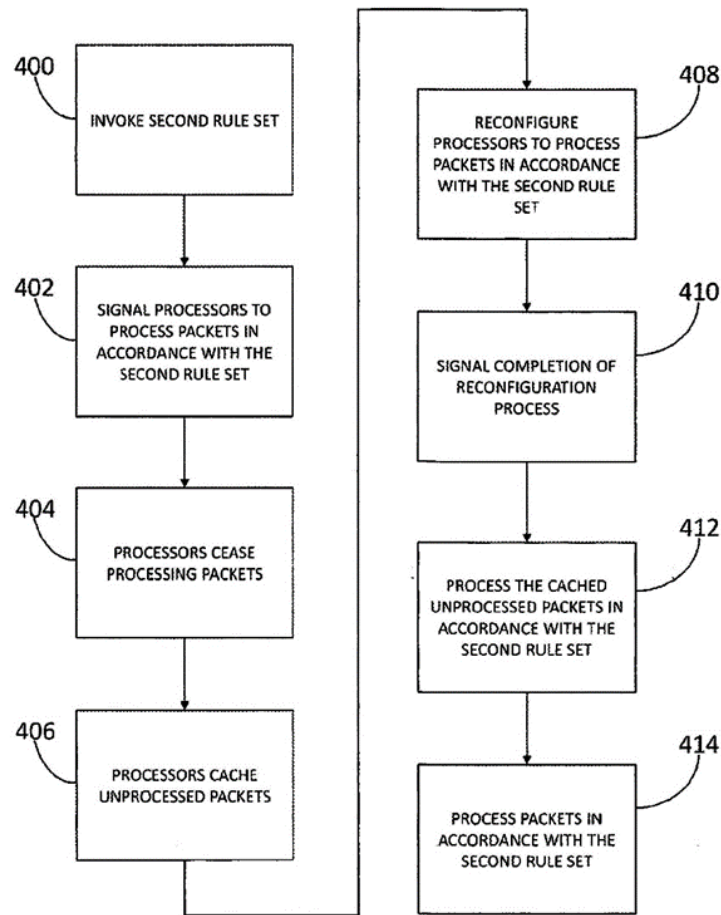


FIG. 4

'806 Patent, Fig. 4. As shown, step 402 reflects the “signal . . . to process packets in accordance with the second rule set.” Then, in steps 404 and 406, the “processors cease processing packets” and “cache [the] *unprocessed packets*” (emphasis added). After reconfiguration, step 412 provides that the system is to “process the cached unprocessed packets in accordance with the second rule set.” It is plain that what is being described is a process in which the system stops processing the packets altogether, rather than only with the first rule set. This is also consistent with how Centripetal’s expert, Dr. Mitzenmacher, described the claim requirements. Tr. 620:1–4 (“So once you’re starting to do the swap for the second rule set, you want to stop processing any packets. Because as you’re doing the update, as the rules are changing, you’re in a state of flux.”).

Centripetal's apparent argument that the cease processing element is satisfied when the accused devices stop processing packets with the old rule set is inconsistent with the claim requirements.

Finally, the Court's finding of non-infringement is further supported by considering the problem that the '806 Patent was designed to address—specifically, that “while implementing a new rule set, a network protection device may continue processing packets in accordance with an outdated rule set.” '806 Patent at 1:25–28. The specification explains that using an outdated rule set “may exacerbate rather than mitigate the impetus for the rule set switch (e.g., the effect of the network attack).” *Id.* at 1:28–31. The cease processing and cache limitations respond to this issue. Specifically, during configuration of a new rule set, the claims indicate that the system stops processing any packets and stores them in a cache to be processed by the new rule set once configuration is complete. '806 Patent at 11:39–53. This solution avoids the problem of processing packets with an outdated rule set while the system is configuring the new rule set.

Critically, Cisco's engineers explained that the problem that the patent was designed to solve—processing packets with an outdated rule set—*still occurs in the accused devices*. *See, e.g.*, Tr. 2518:22–2519:7. Cisco engineer Mr. Shankar explained that he did not view the processing of packets using the old rule set during the “extra few minutes for the firewall to fully program” the new rules to be an issue, as he compared that brief delay to the hours that it takes a human administrator to actually create the new firewall rules (during which time the device would also be processing packets using the old rule set). Tr. 2518:22–2519:7; *see also* PTX-1196 at 007.

For these reasons, the Court FINDS that Cisco's Accused Switches and Routers combined with the DNA Center and Cisco's Accused Firewalls combined with the Firepower Management Center do not literally infringe claims 9 or 17 of the '806 Patent.

### C. Doctrine of Equivalents

Having considered literal infringement, the Court must also determine if the Accused Switches, Routers, and Firewalls still infringe under the doctrine of equivalents. The element the Court ultimately found lacking in the literal infringement analysis above was that the ceasing and caching of the packets did not occur “responsive to” a signal to swap rule sets. Centripetal did not assert that an equivalent of this limitation existed, contending instead that the accused devices satisfied the “preprocessing” element under this doctrine. Centripetal PFF ¶ 301 (arguing that the Accused Switches, Routers, and Firewalls “perform substantially the same function in substantially the same way, to achieve substantially the same result as the ‘preprocessing’ element set forth in the asserted claims”). Centripetal argued that “[s]ubstantially the same function as the ‘preprocessing’ element is performed by receiving information regarding threats, including actions such as blocking and monitoring, which has the same goal of turning information into rules and reprocess them in a format appropriate.” *Id.* (citing Tr. 713:21–714:3). However, Centripetal did not provide any argument under the doctrine of equivalents to establish the causal relationship between the rule switch and the “cease” and “cache” limitations. Moreover, the argument made related to the “preprocessing” element does not relate at all to the “responsive to” element. Accordingly, the Court FINDS that Centripetal has not met its burden to establish infringement under this theory.

## VI. '176 PATENT

### A. Findings of Fact

#### Asserted Claims in the '176 Patent

37. The '176 Patent was issued on January 31, 2017, and has the title “Correlating Packets in Communication Networks.” JTX-3 (“'176 Patent”). The patent was filed on May 15, 2015, and has a priority date of February 10, 2015. Stip. ¶ 21–22.

38. The asserted claims of the '176 Patent are claims 11 and 21. They are, respectively, a system claim and a computer readable media claim. Stip. ¶ 23. Claim 11 is laid out below:

*A system comprising:*

*at least one processor; and*

*a memory storing instructions that when executed by the at least one processor cause the system to:*

*identify a plurality of packets received by a network device from a host located in a first network;*

*generate a plurality of log entries corresponding to the plurality of packets received by the network device;*

*identify a plurality of packets transmitted by the network device to a host located in a second network;*

*generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device;*

*correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and*

*responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:*

*generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and*

*provision a device located in the first network with the one or more rules configured to identify packets received from the host located in the first network.*

'176 Patent at 17:6–35.

39. Claim 11 is identical to claim 21 in every respect except that claim 21 is a computer readable media claim. Claim 21 modifies the introductory preamble language of claim 11 replacing “[a] system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to” with “[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to.” *Id.* at 17:6–9, 18:63–65. For all relevant purposes, the parties treat the two claims the same. Stip. ¶ 25.

40. The '176 Patent addresses the issue of a packet's flow becoming obscured when it passes through a network device. '176 Patent at Title, 1:16–25. A flow refers to a group of packets that contain information distinguishing them from other packets (e.g., each of the packets that comprise an email). *Id.* at 1:18–21. The specification explains that “[n]etwork devices located between endpoints may alter packets associated with a flow and in doing so may potentially obfuscate the flow with which a particular packet is associated.” *Id.* at 1:21–25.

41. Figure 1 of the specification is helpful to understand the problem and the patent's solution:

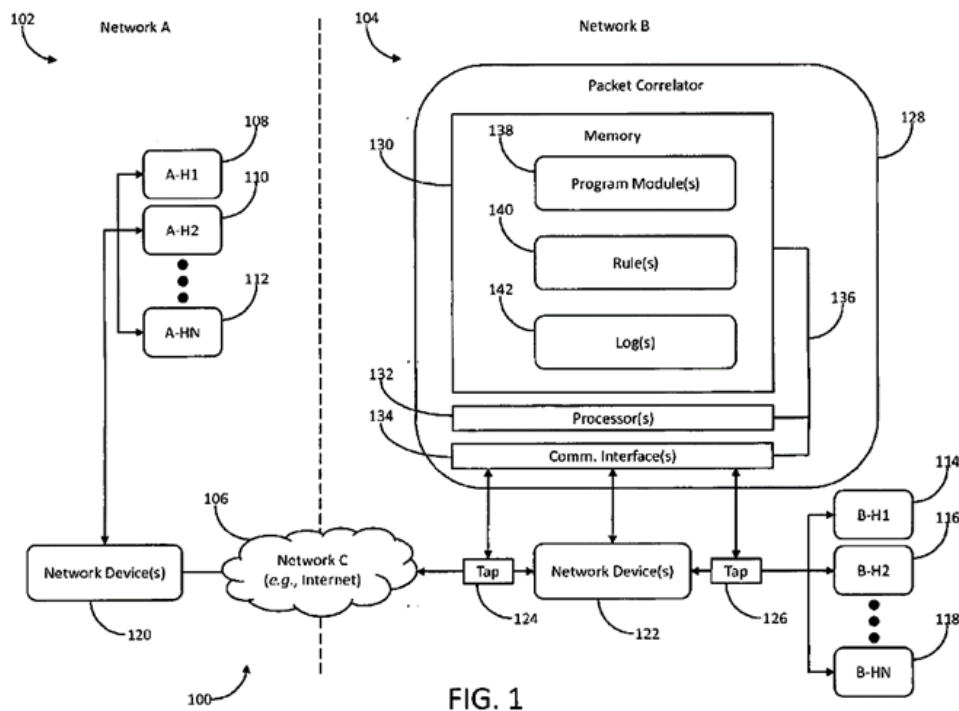


FIG. 1

*Id.* at Fig. 1.

42. The diagram above contains two networks (Network A and Network B) that are connected by a third network (Network C, e.g., the Internet). The endpoints are the host computers in Network A (A-H1, H2, etc.) and the host computers in Network B (B-H1, B-H2, etc.). Packets sent between these two endpoints travel through various network devices, including the network devices labeled 120 and 122.

43. As explained in the specification, when packets enter a network device, the device may “alter one or more aspects of the packets . . . in a way that obfuscates the association” between the packets entering the device from the packets leaving the device, “at least from the perspective of devices other than the network device[.]” *Id.* at 5:14–20. That is to say, packets comprising an email message from host computer B-H1, for example, could pass through network device 122 and become camouflaged, such that other devices in the network would no longer be able to detect that the packets originated from host B-H1.



44. The solution depicted in Figure 1 shows two “taps” (124 and 126) installed on both sides of network device 122 and a corresponding packet correlator (128). The specification explains that in some embodiments, these taps receive packets coming in and out of a network device and generate log records that are sent to the packet correlator. *See, e.g., id.* at 3:60–4:3, 6:13–28. The specification explains that the packet correlator may use the logs to correlate the packets transmitted by the device with the packets received by the network device. *Id.* at 8:46–48. Then, “[r]esponsive to correlating,” the packet correlator may “generate or update” rules used by the tap devices to identify packets coming from a specific source. *Id.* at 12:55, 13:14–18.

45. These general descriptions align with the language of the claims asserted by Centripetal. Specifically, the method outlined in claim 11 provides that the system “identify a plurality of packets *received by a network device* from a host located in a first network” and “generate a plurality of log entries corresponding to the plurality of packets received by the network device.” *Id.* at 17:10–13 (emphasis added). Similarly, the claims provide that the system “identify a plurality of packets *transmitted by the network device* to a host located in a second network” and “generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device.” *Id.* at 17:14–18 (emphasis added).<sup>16</sup> Then, “based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of packets transmitted by the network device,” the system is to “correlate . . . the plurality of packets transmitted by the network device with the plurality of packets received by the

---

<sup>16</sup> Since the language refers to packets “received by a network device” and thereafter refers to actions taken by “*the* network device,” the claims are referring to actions taken by the same network device. *See Convolv, Inc. v. Compaq Comput. Corp.*, 812 F.3d 1313, 1321 (Fed. Cir. 2016) (construing a claim reciting “a processor” and then subsequently referencing functionality for “the processor” to require at least one processor to “perform all of the recited steps” referencing “the” processor).

network device.” *Id.* at 17:19–25. Finally, “responsive to correlating,” the system is to “generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network,” and “provision a device located in the first network with the one or more rules.” *Id.* at 17:26–35. These steps are the same for claim 21. *Id.* at 18:63–19:23.

46. In other words, the claims describe a system responsive to the obfuscation problem identified in the specification. If the network device alters the packets it receives from the computer in the first network before sending the packets to the second network “in a way that obfuscates the association” between the packets, this correlation technique can help identify the packets originating from the first network computer. *See* ’176 Patent at 5:13–20.

The Accused Switches, Routers, and Stealthwatch with Cognitive Threat Analytics

47. Centripetal alleged that Cisco’s Accused Switches and Routers using Stealthwatch with Cognitive Threat Analytics infringe claims 11 and 21 of the ’176 Patent. Tr. 975:17–21, 976:16–19, 995:19–21, 1107:23–1108:10. At trial, Centripetal relied on the infringement opinion of expert witness Dr. Eric Cole and Cisco relied on the non-infringement opinion of expert witness Dr. Kevin Almeroth. Both parties also called a variety of fact witnesses.

48. The Accused Switches and Routers receive and transmit packets using processors and memory storing software instructions. Tr. 477:12–478:14, 484:13–485:3; PTX-1303 at 056; PTX-1313 at 018.

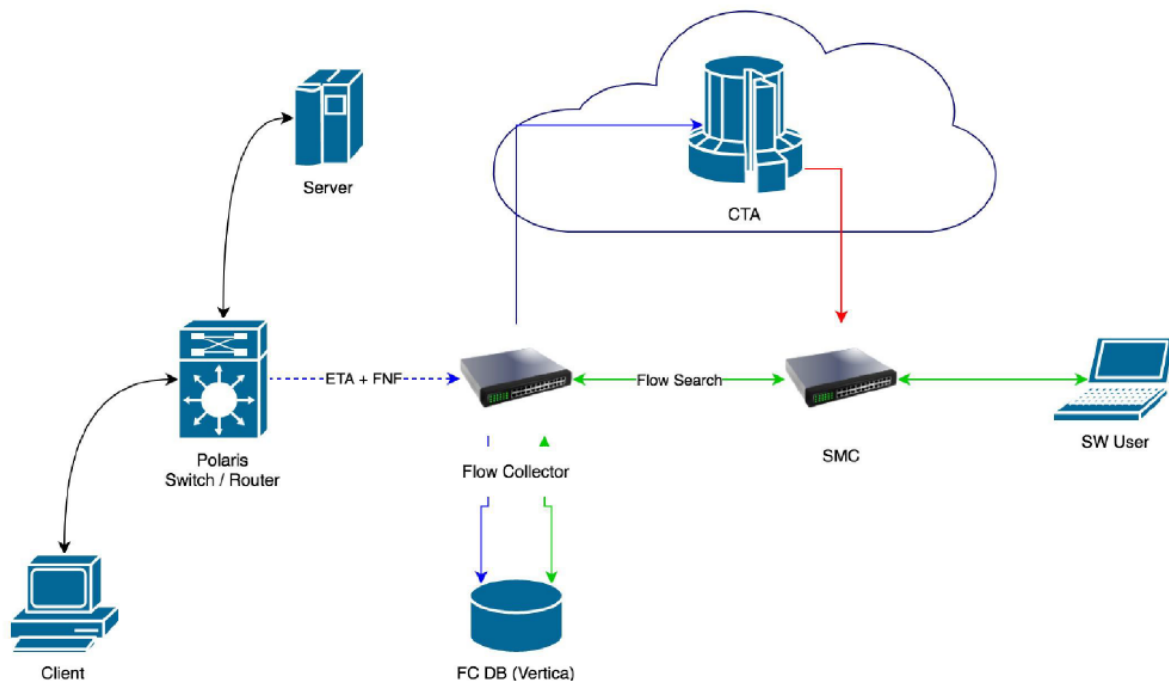
49. As packets transit through the Accused Switches and Routers, the devices can generate NetFlow logs. Tr. 977:18–25, 984:5–13; PTX-1060 at 008. NetFlow is a type of log that contains summaries of information about the packets flowing through the devices. Tr. 984:7–13. NetFlow records can be reported by a switch or router to track “every conversation, or flow, that passes through it. It collects a range of information about these exchanges in a flow record.”

PTX-1417 at 107; *see also* PTX-1060 at 008 (“When processed, NetFlow data can tell you the important details in network transactions’ endpoints of data communication, information about when the conversation occurred, how long it lasted, and what protocols were used.”).

50. The Accused Switches and Routers are capable of exporting NetFlow when the packet enters the device (the “ingress” NetFlow record) and when the packet exits the device (the “egress” NetFlow record). Tr. 986:12–987:1; PTX-1060 at 023; Tr. 2171:23–2172:9, 2180:23–2181:3.

51. The Accused Switches and Routers can be configured to send these NetFlow logs to Stealthwatch, which analyzes traffic flow and monitors for threats. Tr. 998:3–17; PTX-1009 at 009.

52. Centripetal’s witness, Dr. Cole, used the following diagram from Cisco’s technical documentation to depict the accused system:



PTX-1089 at 0979.

53. The diagram shows a “Client” and a “Server” that are communicating with each other through a Cisco switch or router (shown above as the “Polaris Switch/Router”). Tr. 2189:7–18. As packets pass through the switch or router, the device exports NetFlow records to a Stealthwatch Flow Collector. Tr. 2189:19–23.

54. The Stealthwatch Flow Collector analyzes the NetFlow and sends alarms to the Stealthwatch Management Console (labeled as “SMC” above). Tr. 2147:23–2148:7, 2191:8–10. The Stealthwatch Flow Collector can also send information to Cognitive Threat Analytics (labeled as “CTA” above), which analyzes the flow information for malicious activity and can send additional alarms to the Stealthwatch Management Console. Tr. 2189:19–2190:1, 2147:7–22.

55. Cisco indicated that it tells its customers not to export both ingress and egress NetFlow records to Stealthwatch. *See* Tr. 2177:7–12, 2180:15–2181:3; PTX-569 at 282. Cisco engineer Daniel Llewallyn explained that Stealthwatch was built to assume the NetFlow records it ingests are ingress records. Tr. 2171:9–13, 2177:8–10, 2178:22–2179:7 (discussing PTX-569 at 282). If an Accused Switch or Router were to transmit both ingress and egress NetFlow log records to the Stealthwatch Flow Collector, the clear weight of the evidence shows that Stealthwatch does not compare these records to each other. According to Mr. Llewallyn, “[a]ny concept of ingress/egress is gone by the time [the data] gets inside the Stealthwatch flow. . . . [I]t’s just keeping up with how many bytes and packets went in [a] direction.” Tr. 2181:22–2182:4. Cisco’s technical documentation indicates that if a user enables the export of both ingress and egress NetFlow records to Stealthwatch, this “may cause the [Stealthwatch] Flow Collector to double report traffic stats.” PTX-569 at 282; *see also* Tr. 2177:8–2181:3. Additionally, the Stealthwatch Flow Collector contains code directing it to ignore duplicative egress NetFlow records. Tr. 2173:4–8, 2174:3–2175:21, 2177:15–18; DTX-1616 at 443–44, 466; Tr. 2254:11–15 (Dr. Almeroth: “[T]here’s a

variable called ignore egress that attempts to ignore egress records from the same device for which there is already ingress information. And if it is unsuccessful, then it will double count those records erroneously.”).<sup>17</sup>

56. Instead, the record demonstrates that the data analysis conducted by Stealthwatch involves the review of network traffic in order to detect malicious activity, by comparing NetFlow and other types of logging records (such as Syslog or WebFlow) with outside sources of data, such as threat intelligence feeds. *See, e.g.*, PTX-1065 at 005 (“Stealthwatch . . . correlates threat behaviors seen in the enterprise with those seen globally.”). According to Centripetal, “Syslog” is a “type of logging” that proxy sources can send to Stealthwatch, and “WebFlow” is “produced by Syslogs.” Centripetal PFF ¶¶ 351, 382. The Accused Switches and Routers are not proxy sources. *See* Tr. 978:11–18.

57. A human administrator can use the information (i.e., alarms) produced by this Stealthwatch analysis (by interacting with the laptop above labeled “SW User”) to generate new packet-filtering rules to better protect the network. Tr. 2190:2–4; PTX-1089 at 1239. These rules can then issued by the human administrator. Tr. 2190:5–22.

## **B. Conclusions of Law**

Centripetal has not met its burden to establish infringement of the ’176 Patent because it has failed to show by a preponderance of the evidence that Cisco’s technology performs each of the limitations in the claims. Specifically, Centripetal has failed to show that (1) the accused

---

<sup>17</sup> Centripetal points out that Cisco relied on an older, non-accused version of Stealthwatch source code containing the “ignore egress” code. *See* Centripetal PCL ¶ 47. However, the Court does not find this to be a persuasive basis to discredit the evidence. Mr. Llewallyn testified that the ignore egress source code continued to exist in the accused version of Stealthwatch and Centripetal did not present evidence suggesting otherwise. Tr. 2177:15–18; *see also* Tr. 2287:5–2288:19.

technology correlates the packets entering and exiting a network device and that (2) responsive to the correlating, the system generates rules configured to identify packets in a specific network.

Turning first to the correlation limitation, the claims require the system to correlate the “packets received by the network device” with the packets “transmitted by the network device” based on ingress and egress log entries reflecting the received/transmitted packets. ’176 Patent at 17:19–25. Centripetal argued that this claim limitation is satisfied when the Accused Switches and Routers send ingress and egress NetFlow and/or Syslog logs to Stealthwatch, which purportedly correlates the logs “to provide a detailed overview of all traffic that is occurring on the network.” Centripetal PFF ¶ 352. Centripetal also noted that “[Cognitive Threat Analytics], working within Stealthwatch, can leverage the correlations of NetFlow telemetry to detect malicious threats to the security of the network.” Centripetal PFF ¶ 352.<sup>18</sup> Cisco disputed that Stealthwatch is capable of conducting the correlation disclosed by the claims and argued that Centripetal’s expert, Dr. Cole, “provided only conclusory statements without support in any documentary evidence, source code, or Cisco engineer testimony” in support of his correlation opinion. Cisco PFFCL ¶ 262.

The Court agrees with Cisco and finds that Centripetal has not established that the accused technology conducts the kind of correlation specified in the claim language. As an initial matter, it is helpful to first clarify which Cisco logs Centripetal has argued are being correlated by Stealthwatch with Cognitive Threat Analytics. In its Proposed Findings of Fact and Conclusions of Law, Centripetal suggested that the logs can either be NetFlow or other logging records such as Syslog or Webflow. *See* Centripetal PFF ¶ 352 (citing PTX-1065 at 005) (“Stealthwatch correlates NetFlow and/or Syslog information . . . .”); *id.* ¶ 365 (stating that the accused devices “will send

---

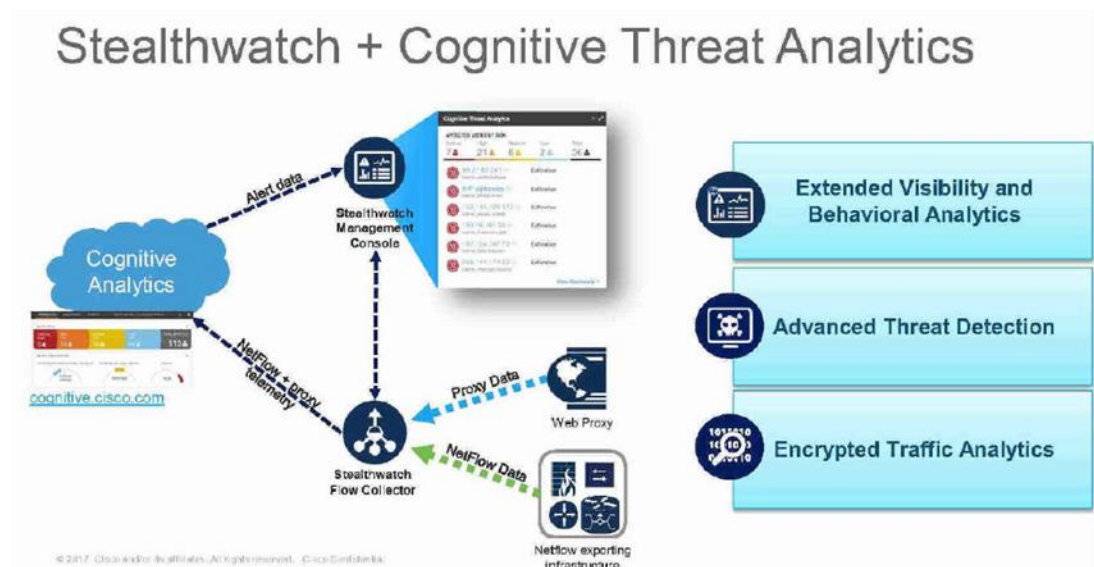
<sup>18</sup> Centripetal’s expert, Dr. Cole, explained that NetFlow telemetry “is just another word for NetFlow log information.” Tr. 997:7–8.

the Netflow logs . . . to Stealthwatch, which will correlate the packet data from packets received and transmitted”); *id.* ¶ 371 (“[Cognitive Threat Analytics] uses the Netflow records that include bidirectional flow and ingress and egress data and correlates this packet data with Webflow . . .”). Centripetal’s infringement expert, Dr. Cole, similarly noted that Syslog records could “fit the logging criteria of the patent language.” Tr. 985:5–8.

Despite these arguments, the record demonstrates that Centripetal’s infringement theory can only be understood to relate to the correlation of ingress and egress *NetFlow* records. Importantly, Dr. Cole’s infringement opinion only relied on Stealthwatch’s alleged correlation of ingress and egress NetFlow. *See, e.g.*, Tr. 993:19–999:15 (Dr. Cole’s direct examination explaining how NetFlow meets the “correlate” claim element); Tr. 1102:16–1103:4, 1106:5–8, 1108:1–5 (Dr. Cole: “[T]he important thing for me are the ingress and egress Netflow data. There’s nothing in the claim that’s exclusive to just those two, so there can be other data in there as long as those two NetFlow records are being correlated.”); Tr. 1116:23–1117:1 (Dr. Cole: “This shows that the claim language says it must be able to correlate the two NetFlows. So this is confirming that it can correlate NetFlow by itself which would consist of ingress and egress NetFlows.”). Dr. Cole also noted that his infringement theory did not involve a proxy, meaning that any correlation by Stealthwatch of Syslogs or WebFlow, which Centripetal indicated are generated by proxy sources, does not support Dr. Cole’s infringement analysis. *See* Tr. 978:11–18 (“[W]ith the ’176 patent, there’s actually not a proxy in the claim language. So we don’t actually have a proxy in this case.”). And finally, Centripetal’s counsel largely conceded at the Rule 63 hearing that its infringement theory involved only the correlation of ingress and egress NetFlow records. *See* R. 63 Tr. 482:5–25 (“[T]he evidence shows that the NetFlow data—that’s what we focused on—that was infringing. . . . So if we had a different claim construction, we might look at the proxy data. We

may have alternative theories. We may have [S]yslog, and we have other stuff. . . . I think the evidence shows that the NetFlow data is what we’re accusing of infringing.”). For these reasons, the Court will consider only whether the evidence shows that ingress and egress *Netflow* records are correlated by Stealthwatch with Cognitive Threat Analytics.

Dr. Cole testified that he relied on testing, a review of Cisco source code, and Cisco documents in reaching his opinion that ingress and egress NetFlow records are correlated by Stealthwatch with Cognitive Threat Analytics. Tr. 999:7–15. Despite this assertion, at trial Dr. Cole did not discuss the correlation testing or point to specific pieces of source code showing correlation.<sup>19</sup> See Tr. 993:19–999:15 (Dr. Cole’s direct testimony on the “correlate” claim element). Because of this, the Court focuses on the three Cisco documents that were discussed by Dr. Cole. First, Dr. Cole relied on a diagram that depicts NetFlow data and Proxy data being sent to the Stealthwatch Flow Collector:



<sup>19</sup> To be clear, Dr. Cole discussed his testing and relied on other Cisco documents in support of his opinions as to other elements of the claims, for example that the Accused Switches and Routers can be set to report both ingress and egress NetFlow records. See, e.g., 981:7–993:18 (Dr. Cole’s direct testimony on the “identify” and “generate” claim elements).



PTX-1065 at 005. Below the diagram, the document also includes explanatory language noting that “Stealthwatch . . . correlates threat behaviors seen in the enterprise with those seen globally” and that the “[c]ustomer may use either NetFlow or proxy data, or both.” *Id.*

While this document indicates that Stealthwatch engages in correlation, it does not show the kind of correlation required by the claim language. The claim requires a correlation of “packets transmitted by the network device” with “packets received by the network device” based on the ingress and egress log entries corresponding to those sets of packets. ’176 Patent at 17:19–25. Instead, the diagram above depicts a combination of “NetFlow Data” and “Proxy Data,” and the explanatory text describes correlation of internal and external threat behaviors.

Dr. Cole opined that the document showed that Stealthwatch engages in the claimed correlation because the document states that a “[c]ustomer may use either NetFlow or proxy data or both.” Tr. 1116:6–1117:1; PTX-1065 at 005. Dr. Cole said that this indicated “customers can just use NetFlow by itself to do that correlation. It does not need to use the proxy data.” Tr. 1116:12–13. Dr. Cole’s opinion is contradicted by the evidence. As explained above, the text accompanying the diagram explains that Stealthwatch “correlates threat behaviors seen in the enterprise with those seen globally.” PTX-1065 at 005. This capability is markedly different than correlating packets entering and exiting a network device using ingress and egress NetFlow records. The document’s statement that a “[c]ustomer may use either NetFlow or proxy data or both,” considered in context, is better understood to mean that the customer may correlate external threat behaviors with NetFlow, proxy data, or both Netflow and proxy data.

Additionally, Dr. Cole relied on language in two different versions of Stealthwatch release notes that referenced correlation:

[Cognitive Threat Analytics] can now leverage detections from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from

Stealthwatch. This is accomplished by the system through correlation of both telemetry types. According to measurements by Cisco, the number of both confirmed and detected threats should increase by approximately 10%[.]

PTX-591 at 522; *see also* PTX-1009 at 009. Dr. Cole opined that “[r]eading this entire document and all the other pieces of evidence, this is one piece, in my opinion, [that] supports that [Cognitive Threat Analytics] not only correlates the WebFlow and the NetFlow, but also the NetFlow data is also correlated among itself.” Tr. 1109:11–14; *see also* R. 63 Tr. 484:3–11. Dr. Cole did not provide any support for this opinion beyond claiming that “somebody who has read the entire document would understand that it would mean WebFlow, NetFlow and NetFlow among itself.” Tr. 1109:17–19.

Given the paucity and indefiniteness of the evidence Dr. Cole relied on, the Court gives little weight to his opinion that Stealthwatch is capable of correlating ingress and egress NetFlow records. Moreover, the Court’s conclusion is bolstered by the evidence presented by Cisco showing that the opposite is true. First, Cisco’s technical documentation indicates that if a user enables the export of both ingress and egress records to Stealthwatch, this “may cause the [Stealthwatch] Flow Collector to double report traffic stats.” PTX-569 at 282. Second, if a customer were to export both, the Stealthwatch Flow Collector contains code directing it to ignore duplicative egress NetFlow records. Tr. 2173:4–8. Third, consistent with this understanding, Cisco engineer Daniel Llewallyn explained that Stealthwatch was built to assume all the NetFlow records it ingests are ingress records. Tr. 2171:9–13. And finally, Mr. Llewallyn explained that even if both ingress and egress records were collected by Stealthwatch, that distinction is lost before any correlation could occur. Tr. 2181:14–2182:15 (“Any concept of ingress/egress is gone by the time it gets inside the Stealthwatch flow. . . . [I]t’s just keeping up with how many bytes and packets went in this

direction.”). For these reasons, the Court finds that Centripetal has not shown that the accused system practices the correlation limitation.<sup>20</sup>

This conclusion is further supported by considering the problem that the ’176 Patent was designed to solve—packet obfuscation by a network device. *See* ’176 Patent at 5:14–20 (stating that a network device may “alter one or more aspects of the packets . . . in a way that obfuscates the association” between the packets entering the device from the packets leaving the device, “at least from the perspective of devices other than the network device[]”). Importantly, it is the *network device* doing the obfuscation, thwarting other network devices from identifying packets associated with a particular source. But in the accused Cisco system, the network device is a *Cisco device*. Cisco’s expert, Dr. Almeroth, explained that because Cisco controls the network device (i.e., the Accused Switches and Routers), Cisco is capable of seeing any changes to the packets made by it. Tr. 2297:12–2298:15. For that reason, Cisco need not rely on correlation to determine what is happening inside of the device. *See* Tr. 2297:21–24 (comparing the network device to a tunnel into which a fleeing car may travel in order to change its appearance during a period of no visibility, and explaining that in this “analogy, Cisco is the tunnel” and “[t]hey actually have someone in the tunnel watching the cars, and they can actually see when somebody jumps out of a car and gets into another”). Given this functionality, the Accused Switches and Routers do not have the problem that the ’176 Patent was designed to solve.

---

<sup>20</sup> After Centripetal rested its infringement case, it called an invalidity expert, Dr. Trent Jaeger, who put forward a different interpretation of the ’176 Patent claim elements—specifically, that the claim language does not require ingress and egress NetFlow records to refer to the same network device because of the reference in the claim language to “one or more network devices.” Tr. 3157:16–23. This is not persuasive. Given that the claim language first refers to “a network device,” and then recites requirements of “the network device,” all of the claim requirements of “the network device” must be satisfied by a single network device to infringe. *See supra* note 16.

The Court also finds that Centripetal has failed to provide sufficient evidence that the accused technology “generate[s], based on the correlating, one or more rules configured to identify packets received from the host located in the first network” or “provision[s] a device” with those rules. *See* ’176 Patent at 17:29–31. Centripetal argued that this claim limitation is met because Stealthwatch with Cognitive Threat Analytics generates alerts that are sent to the Stealthwatch Management Console. Tr. 1113:17–1114:6, 1001:1–7, 1002:4–1003:21, 1005:4–19, 1112:18–1113:8. This functionality, however, does not meet the claim limitation.

Specifically, Centripetal has failed to show that the accused system generates and provisions *rules* responsive to the correlating to identify packets in a specific network. While the evidence shows that the system generates alerts, these alerts are not “rules,” as the term is defined by the Court’s claim construction order. *See Markman* Order at 9 (adopting the parties’ agreed construction that a rule is “a condition or set of conditions that when satisfied cause a specific function to occur”). Centripetal’s expert, Dr. Cole, referred to the quarantine command issued by Cisco’s Identity Services Engine (discussed above in relation to the ’193 Patent) as a “rule” that could be generated by Stealthwatch. Tr. 1002:4–1003:1. However, an Identity Services Engine quarantine must be manually initiated by a human administrator. Tr. 2267:13–2268:4, 2300:21–2301:13, 2185:22–2188:5. In contrast, the claims refer to the system itself generating rules based on the correlating, not a human. ’176 Patent at 17:29–31. Further, Centripetal has not shown that the rules that would be created based on a Stealthwatch alert would have the ability to “identify packets received from the host located in the first network,” as required by the claim language. *Id.* at 17:29–31; *see also* Tr. 2265:2–22.

For these reasons, the Court finds that Centripetal has failed to establish both the correlation limitation and the limitation requiring generation of rules responsive to the correlating.

Accordingly, the Court FINDS that Cisco's Accused Switches and Routers, using Stealthwatch with Cognitive Threat Analytics, do not literally infringe claims 11 or 21 of the '176 Patent.

### C. Doctrine of Equivalents

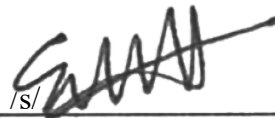
Centripetal acknowledged that it did not present any evidence to establish infringement of the '176 Patent claims under the doctrine of equivalents. Tr. 1088:2–7 (“We did not put in evidence of doctrine of equivalents with Dr. Cole. We believe there is literal infringement on this, and doctrine of equivalents is not necessary for these patents.”). The patentee bears the burden of proving equivalence. *Carroll Touch Inc. v. Electro Mech. Sys, Inc.*, 15 F.3d 1573, 1578–79 (Fed. Cir. 1993). As such, and given Centripetal's concession, the Court FINDS that Centripetal has not met its burden to establish infringement under the doctrine of equivalents.

## VII. CONCLUSION

For the reasons set forth above, the Court FINDS that Centripetal has failed to prove infringement of the '193, '806, or '176 Patents by a preponderance of the evidence.<sup>21</sup> Therefore, the Court need not reach issues related to patent validity or damages. Finding “no just reason for delay,” the Court DIRECTS the Clerk to enter partial final judgment in favor of Cisco pursuant to Rule 54(b) of the Federal Rules of Civil Procedure.

The Clerk is REQUESTED to send a copy of this Memorandum Opinion and Order to all counsel of record.

It is so ORDERED.



\_\_\_\_\_  
Elizabeth W. Hanes  
United States District Judge

Date: December 11, 2023

---

<sup>21</sup> Having found that Centripetal has failed to establish the limitations discussed above, the Court does not find it necessary to address Cisco's other arguments regarding Centripetal's alleged failure to meet the additional elements of direct and indirect infringement.